ENHANCING THE GOVERNANCE OF INFORMATION SECURITY IN DEVELOPING COUNTRIES: THE CASE OF ZANZIBAR

by

Hussein Khamis Shaaban

A thesis submitted to the University of Bedfordshire, in partial fulfilment of the requirements of the degree of Doctor of Philosophy

January, 2014

ABSTRACT

Organisations in the developing countries need to protect their information assets (IA) in an optimal way. This thesis is based upon the argument that in order to achieve fully effective information security management (ISM) strategy, it is essential to look at information security in a socio-technical context, i.e. the cultural, ethical, moral, legal dimensions, tools, devices and techniques. The motivation for this study originated from the concern of social chaos, which results from ineffective information security practices in organisations in the developing nations. The present strategies were developed for organisations in countries where culture is different to culture of the developing world. Culture has been pointed out as an important factor of human behaviour. This research is trying to enhance information security culture in the context of Zanzibar by integrating both social and technical issues.

The theoretical foundation for this research is based on cultural theories and the theory of semiotics. In particular, the study utilised the GLOBE Project (House et al, 2004), Competing Values Framework (Quinn and Cameron; 1983) and Semiotic Framework (Liu, 2000). These studies guide the cultural study and the semiotics study. The research seeks to better understand how culture impact the governance of information security and develop a framework that enhances the governance of information security in non-profit organisations. ISO/IEC 27002 best practices in information security management provided technical guidance in this work.

The major findings include lack of benchmarking in the governance of information security. Cultural issues impact the governance of information security. Drawing the evidence from the case study a framework for information security culture was proposed. In addition, a novel process model for information security analysis based on semiotics was developed. The process model and the framework integrated both social and technical issues and could be implemented in any non-profit organisation operating within a societal context with similar cultural feature as Zanzibar. The framework was evaluated using this process model developed in this research. The evaluated framework provides opportunities for future research in this area.

DECLARATION

I declare that this thesis is my own unaided work. It is being submitted for the degree of Ph.D. at the University of Bedfordshire.

It has not been submitted before for any degree or examination in any other University.

Name of candidate: Hussein Khamis Shaaban Signature:

Date:

DEDICATION

I dedicate this work to my extended family. Their pride, encouragement, patience and support during my endeavours made this work achievable.

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

ACKNOWLEDGEMENTS

I thank my Director of Studies, Dr Marc Conrad, for believe in me, invaluable guidance, patience, encouragement and support in my research endeavours. I would like to thank my second supervisor, Dr Tim French, for his insight.

Also, I would like to thank my examiners, Dr Paul Sant and Dr Simon Polovina (Sheffield Hallam University), for their valuable feedback on my thesis. My gratitude for feedback on my transfer/mock viva given to me by Dr Gregory Epiphaniou, Dr Haider Al-Khateib, Dr Marcia Gibson and Dr Mitul Shukla.

I would like to thank the University of Bedfordshire staff especially Dr Moira Hampson and Prof Angus Duncan for their support.

I would like to thank the Office of the Second Vice President of Zanzibar for permission to conduct research in Zanzibar, and voluntary participation of numerous employees of Zanzibar's public sector in the data collection process.

This research was funded by the United Republic of Tanzania and the State University of Zanzibar under the World Bank Grant for Science Education.

PUBLICATIONS FROM THIS THESIS

The work discussed in this thesis has led to the following publications.

1. Shaaban, H., Conrad, M. and French, T. (2012) 'Towards a framework for managing information security in Zanzibar's public organisations: a developing country's view', *IADIS Conference,* Berlin, Germany, 10-13 March 2012.
2. Shaaban, H., Conrad, M. and French, T. (2012) 'State of information security in Zanzibar's public organisations', *IST-Africa 2012,* Dar es Salaam, Tanzania, 9-12 May 2012.
3. Shaaban, H. and Conrad, M (2013) 'Democracy, culture and information security: a case study in Zanzibar', *Information Management & Computer Security,* 21(3), pp. 191-201.
4. French, T., Conrad, M. and Shaaban, H. (2013) 'Localized trust – the semiotics in culture and e-culture', *International Journal of Digital Society,* special edition 1(1), pp. 817-825.

CHAPTER 1

1 INTRODUCTION

Information Systems (IS) in organisations – already ubiquitous in developed countries – are being deployed in developing countries more and more: services such registration of birth and death, issue of passport, registration of marriage, collection of tax, registration of voters, payroll, and public finance amongst others have been computerised or are under active considerations for automation. Securing these services has become a vital function within the information system governance establishments. With an increased dependence on the IS connected over open data networks, efficient information security governance has become a crucial success feature for organisations in the developed or developing countries alike. Developing countries are going through processes that developed countries went through many years ago. In order to achieve effective information security governance, it is essential to develop and implement effective information security governance based on a local context. The focus of this research is to enhance information security governance in non-profit organisations in the context of a developing country.

According to (United Nations, 2008) developed countries are Canada, the United States, Japan, Australia, New Zealand, and European countries, while the remainder are developing countries. The adoption of information systems faces many challenges in many developing countries such as lack of skilled personnel (Cheang and Sang, 2009; Mundy and Musa, 2010; Karokola and Yngström, 2009; Kimwele, Mwangi and Kimani, 2010), financial constraint (Karokola and Yngström, 2008; Kimwele, Mwangi and Kimani, 2010), national culture, and inferior infrastructures (Cheang and Sang, 2009; Mundy and Musa, 2010; Karokola and Yngström, 2009) among others. Past studies have indicated social issues are at least as vital as technical issues in implementing information security governance (Dhillon and Torkzadeh, 2006; Siponen and Oinas-Kukkonen, 2007).

An information system (IS) is defined as "A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information" (CNSS, 2010; p.37). It also includes industrial/process controls equipment, equipment for telephone switching and exchange; and equipment for environmental control (CNSS, 2010).

1.1 Overview of the research problem

The discipline of information security is concerned with the confidentiality, integrity and availability of information assets. There are several unsolved issues related with efficient information security governance in the developing countries such as voter registration, voting, passport, national identity, financial records and education records.

The present information security governance studies seek to tackle some of these issues; however, most of these studies argue within a culture of western societies. These studies may not be applicable to societies outside the west.

This research is concerned with improving information security governance in an organisation that resides in a culture outside the Western society, specifically Zanzibar. The main research question is:

RQM. *What organisational factors need to be tackled or managed to develop and implement effective information security governance in the context of Zanzibar?*

1.2 Research Purpose

The purpose of this research is:
To develop a useful, integrated and theoretically robust framework that will support non-profit organisations to succeed in the challenging task of improving quality information security governance within the context of Zanzibar. The objectives of the research are to:

- Understand the existing information security strategies
- Understand the current state of information security in non-profit organisations
- Understand the cultural factors which may impact development and implementation of information security governance
- Develop a framework for improving information security culture in the Zanzibar context

1.3 Research Motivation

The researcher has experienced the deployment of IS at various organisations in Zanzibar and how the adopted IS have transformed the way services are provided. However, the researcher has doubted the sustainability of IS usage in Zanzibar and other developing countries in general. As more countries are connected through open networks and IS usage increases so do criminal activities on information systems (Lee, 1997). Many developing countries have experienced information security breaches. Some public institutions in Tanzania have been victims of cyber attacks including Tanzania National Bureau of Statistic, the Tanzania Parliament, Tanzanian Revenue Authority and Bank of Tanzania (Mutarubukwa, 2010). Another incident occurred when two Bulgarian nationals were caught stealing at Automatic Teller Machine (ATM) in Dar es Salaam (Juma, 2009). Since the introduction of multi-party democracy in Zanzibar in 1992, elections have been marred with claims of ballot rigging. Tanzania is not the only developing country to face information security breaches. Hackers succeeded to deface a website of Ministry of Environment of Cambodia (Cheang, 2009). In Zanzibar, majority of employees work in a non-profit sector. The researcher as an employee of in this sector did observe that computer users in this sector have only fear of losing their data to viruses. The researcher as an IS professional would like to see this trend in security vulnerability for organisations in developing countries to be halted. The current thesis helps in this by identifying the cultural factors that influence governance of information security and develop a framework that will enhance management of information security in the non-profit organisations.

1.4 Research Questions

The research work presented in this thesis addresses the study purpose and the study objectives through the following research questions:

RQ1. What are the existing information security strategies?

RQ2. What is the current state of information security governance in non-profit organisations in the context of Zanzibar?

RQ3. What are the cultural factors that impact upon information security governance in non-profit organisations in the context of Zanzibar?

RQ4. How can non-profit organisations improve their information security governance in the context of Zanzibar?

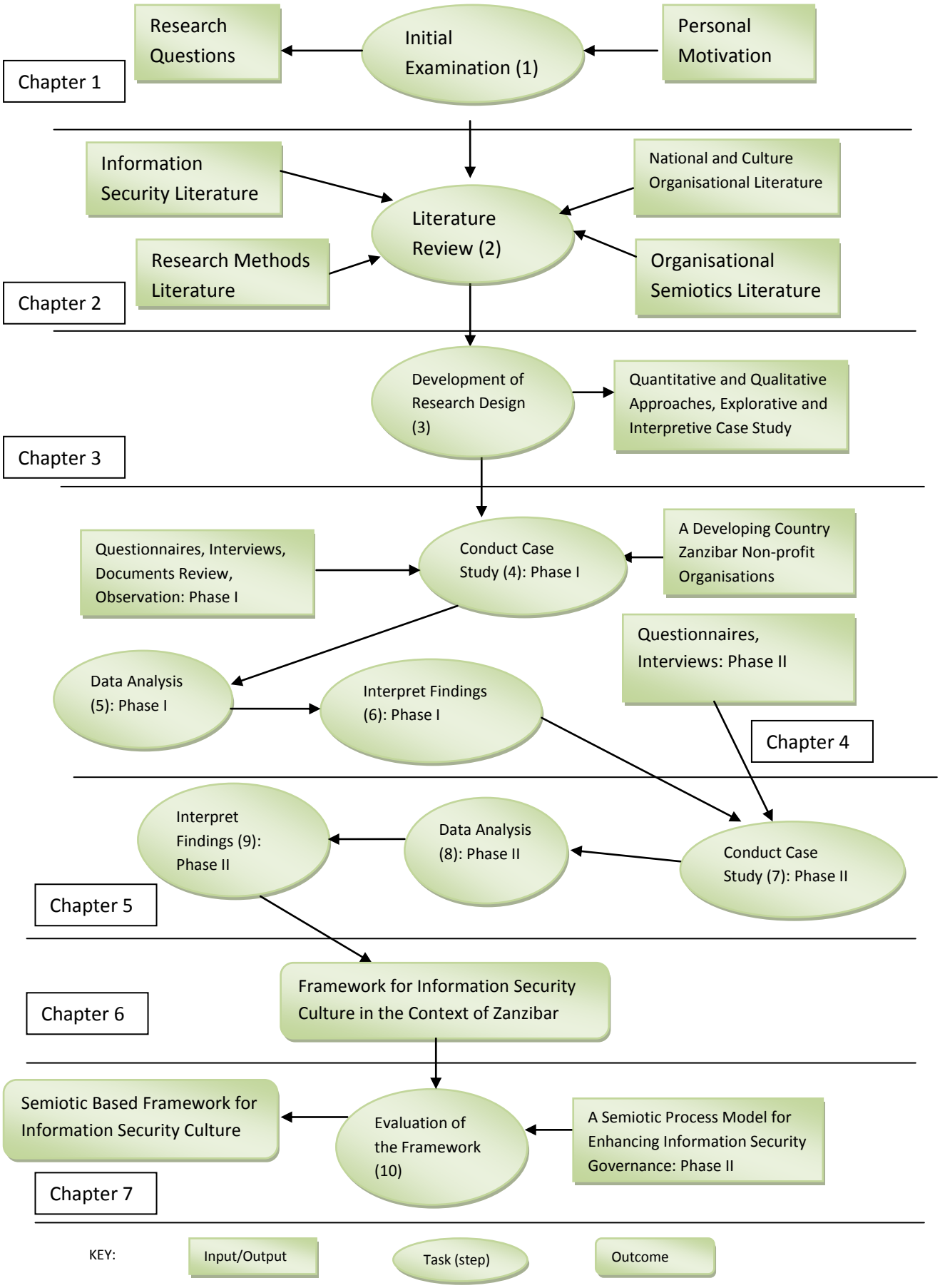

Figure 1.5.1: Research Process

An approach of mixed methods consisting of quantitative and qualitative approaches will be employed in this research work to address the research questions. This will, in turn, seek to achieve the research objectives, realise the research purpose and bring about a better understanding of the research problem.

1.5 Overview of the research process

This investigation went through a series of processes as described in the Figure 1.5.1. An exploratory case study was performed, consisting of several organisations. Data collection and analysis was conducted using a mixed methods approach. The details of the research processes are presented in Chapter 3.

1.6 Research Benefits

This research will be relevant to non-profit organisations such as public sector organisations in the developing countries. The benefits of this thesis include:

- A process model for enhancing information security governance grounded by the theory of semiotics for organisations in the developing countries.
- A framework for information security culture for organisations in the developing world.
- A contribution to the knowledge of non-profit organisations concerning their state of information security governance in the developing countries.
- A contribution to the knowledge concerning integrating social and technical issues in developing model for information security governance.
- A contribution to the knowledge concerning cultural factors, which may influence information security governance in the Zanzibar context.
- Present an analysis of information security governance processes and information security culture in the context of Zanzibar.
- Present a healthy foundation for further research into information security governance in the developing countries.
- An awareness of the information security needs of non-profit organisation in the developing countries.

1.7 Research Focus

The focus of this thesis is on the factors relevant to the management of information security in non-profit organisations in the developing countries. The issues that are considered peripheral to the focus of this thesis are:

- Activities and factors associated with information security governance within organisations in a developing country environment.
- Issues related to information security culture in organisations in the context of a developing country.
- Technical issues of information security in organisations in the context of a developing country.

1.8 Potential Limitations

The potential limits of the research are:

- The research project is focused on non-profit organisations which are in public sector. The findings may not be appropriate for organisations in a different cultural context.
- The organisations happened to be in different fields and sizes.
- The research had smaller population of participants and conclusions are drawn from on data collected in Zanzibar.

1.9 Layout of the Thesis

Chapter 1 has presented the research problem and the research infrastructure including the research purpose, objectives, the research questions and approach.

Chapter 2 discusses the literature review. It provides the foundations of the research.

Chapter 3 is the discussion of the research methodology.

Chapter 4 presents the data analysis and research findings for Phase I of the research.

Chapter 5 is a presentation of the data analysis and research findings for Phase II of the research.

Chapter 6 discusses recommendations for improving information security in the form of a framework of information security culture.

Chapter 7 discusses recommendations for refining the framework for information security culture in the form of a semiotic process for information security governance.

Chapter 8 is a discussion of conclusions of the thesis.

1.10 Summary

This chapter has presented the research problem and the research infrastructure including the research purpose, objectives, the research questions and the approach taken to the research project. The chapter concludes with an overview of the potential limitations of the research project.

In the next chapter, Chapter 2, the relevant literature is discussed which provides the theoretical foundation of this research.

CHAPTER 2

2 THE LITERATURE REVIEW

2.1 Introduction

This chapter introduces the literature on the relevant areas of the research project; information security management practices, ICT in the developing countries, culture, organisational semiotics, and relevant features of Zanzibar. The aim of literature review is to highlight gaps in the literature concerning information security management in non-profit organisations in the developing countries and provide background information on the literature that is used to form the theoretical framework for the research project.

2.2 Information Security Background

2.2.1 Definition of information security

According to CNSS (2010, p.37), information security is "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". The foundation of information security consists of the three properties which are confidentiality, integrity and availability (Bishop, 2003, p.3; Pfleeger, 1997). In this thesis, information security is defined as "preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved" (BSI, 2007; p.1). The properties of information security are defined below:

- Confidentiality means that information is disclosed to an authorised user.
- Integrity means information is not modified by an unauthorised user.
- Availability means information is available when required to an authorised user.

- Authenticity means a user attempting to access the information is in fact the user to whom the level of access belongs.
- Accountability means the user is responsible to the safeguarding of the information the user accesses.
- Non-repudiation means a sender of information cannot denies having sent the information.
- Reliability means information is being consistently processed according to its design.

2.2.2 Threats on information systems

In order to provide protection we need to provide certain measures according to a threat that information system is facing. A threat is a cause of harm to an organisation. Threats could be caused by external or internal sources including but not limited to employees actions, act of nature, malicious codes, technical failures, deliberate attacks and competitors (Whitman and Mattord; 2005, Posthumus and von Solms; 2004). Attacks could be in the form of automated attacks or combination of social engineering and automated attacks (Radiant and Gonzalez; 2007).

Threats target vulnerabilities in an information system to cause damage. Vulnerability is a weakness of an information system that can be exploited by a threat (BSI, 2007). Vulnerabilities could be unsecured ICT equipment, weak password, immature software, untrained employees and weak physical security, among others.

A social engineering attack is a technique where an attacker employs tactics to leverage human trust on the targeted system to acquire confidential information. Phishing is an example of a social engineering attack in which an attacker sends an email to an individual alleging to come from a trusted source, such as a free email provider such as Hotmail or Yahoo. The email requests that the user reply with account information and the user's account password, so the trusted source can verify the correct functioning of the account.

Some attackers send unsolicited emails in bulk to recipients. These emails are called Spam. These emails might cause congestions in a network. Spam emails might be for adverts, scam, charity, offers et cetera.

Malicious code or software is abbreviated as malware, which is designed to penetrate information systems to execute malicious actions without the owner's consent (Skoudis

and Zeltser, 2003). There are various categories of malware. A rootkit (Butler et al., 2008) is a category of malware in which an attacker utilises the software to maintain access to a violated system. A spyware is a category of malware which can be utilised by an attacker to gather information about the user. A spyware can be made to secretly record the user's keystrokes of a keyboard, for example. A computer virus is another category of malware. A virus is a program that duplicates itself in a computer without the owner's consent or awareness. A virus could damage or erase data on a computer, execute an email program to spread itself to other computers, or even delete everything in a hard disk.

Automated attacks are used by attackers trying to find vulnerabilities in information systems or gather email addresses for spam. A dictionary attack is an example of an automated attack that performs guessing process using words from a dictionary to crack a password. Ophcrack v3.4.0 software uses dictionary attack to crack a password with up to 14 characters with a combination of numbers, small letters, and capital letters (Fisher, 2013).

As mentioned earlier, there are threats that originate from inside an organisation. Employees can access confidential information through authorised access, unauthorised access or accidental access during their daily activities. Employees who have the knowledge of information system infrastructure of their organisations are significant insider threats. In this thesis, an insider threat is defined as "threats originating from people who have been given access rights to an IS and misuse their privileges, thus violating the IS security policy of the organisation" (Theoharidou et al., 2005, p.473).

There has been a rapid rise in phishing attacks. According to the BBC there was an 8000 percent increase in phishing attacks in 2006 (BBC, 2006). A Chinese hosted phishing scam targeted Facebook in 2007 (Singel, 2008). A major job search site Monster.com was victim to a phishing scam originating in Turkey in July 2008 (Savvas, 2008). A survey by Ernst & Young (2009) has indicated that 41% of respondents experienced an increase in external attacks and 25% of respondents experienced an increase in internal attacks. Also, in the same survey, 19% of respondents experienced external perpetrated crime and 13% of respondents experienced internal perpetrated crime. In 2006 Computer Crime and Security Survey by Computer Security Institute/Federal Bureau of Investigation identified insider abuses as among the top incidents reported by organisations (CSI, 2006).

There has been a large number of IS users who fell for phishing attacks on their systems. According to Sheng (2010), 90% of respondents had given information on phishing website they had clicked. In a survey by Computer Security Institute, it was reported that 67.1% of respondents had experienced malware infection (CSI, 2011). 31% of respondents believe that their IT security team had been kept awake by unauthorised users (CISCO, 2010). According to survey by PWC (2013) public sector organisations are defending yesterday's threats. In other words, public sector organisations have information assurance methods which are not up to date. In the same survey, it has been reported that security incidents have increased by 15% while the financial losses caused by the same security incidents have drastically increased by 101%.

2.2.3 Countermeasures against threats

In order to provide protection, countermeasures must be implemented according to threats that organisations are facing. Measures that are implemented to guarantee the protection of confidentiality, integrity and availability of information systems are called information assurances. Some examples of countermeasures that are used to protect against threats are:

- Training and awareness administered to employees to limit employees' actions that could jeopardise security of information systems.
- Use of strong passwords in authentication scenarios.
- Use of backup systems to protect against an act of nature.
- Use of anti-virus, anti-malware, anti-spam software to protect against virus, malware and spam attacks.
- Use of information security management standards to benchmark the security activities in an organisation.
- Image verification, mod rewrite, black hole, request limitation, hidden field trap, and spider trap among others can be used to protect from automated attacks (Kadakia, 2013).

2.3 Information security in developing countries

Developing countries are those countries which are in a process of industrialisation but have limited resources (Odedra and Madon; 1993). According to (United Nations, 2008) developed countries are Canada, the United States, Japan, Australia, New Zealand, and European countries, while the remainder are developing countries (which indeed classifies apparently wealthy countries such as Saudi Arabia as developing countries).

Many developing countries are in an early stage of adopting information systems in their government institutions (Karokola and Yngström, 2009). The adoption of information systems faces many challenges in many developing countries such as lack of skilled personnel (Cheang and Sang, 2009; Mundy and Musa, 2010; Karokola and Yngström, 2009; Kimwele, Mwangi and Kimani, 2010), financial constraint (Karokola and Yngström, 2008; Kimwele, Mwangi and Kimani, 2010), national culture, and inferior infrastructures (Cheang and Sang, 2009; Mundy and Musa, 2010; Karokola and Yngström, 2009) among others.

Furthermore, information security programs in many organisations in developing countries are not part of strategic plans nor are they operational (Bakari et al., 2005), they lack documentation (Bakari et al., 2005; Kimwele, Mwangi and Kimani, 2011), and lack benchmarking (Bakari et al., 2005). Lack of user awareness, and culture in security is another challenge facing developing countries (Karokola and Yngström, 2008; Kimwele, Mwangi and Kimani, 2010). Many organisations in developing countries do not have recognised information security strategies (Abu-Musa, 2010). Also, many organisations lack backup and business continuity plans (Abu-Musa, 2010; Kimwele, Mwangi and Kimani; 2011).

Training and awareness in information security is expensive, and there is a challenge in its delivery (Tarimo et al. 2006). In the literature, it has been reported that cultural aspects, management support, budgetary constraints, lack of national level information security policies and guidelines, and lack of motivation to employees are hindrances to information security awareness initiatives in organisations (Casmir and Yngström, 2005).

Many developing countries lack a necessary legal framework at the national level for digital information security (Bakari, et al., 2005; Karokola and Yngström 2008), or they are at the development stage for legislation that protect e-commerce (Ulanga, 2005). There is weak law enforcement in many developing countries on crimes against information systems (Ndou, 2004). This is due to lack of skills by law enforcement agencies on these types of crimes, corruption and lack of proper legislation. Nour et al. (2007) suggested that in an environment of low level of democratisation initiatives and low level of ICT preparation; privacy, security, and confidentiality issues would have little importance.

2.4 Information security management

There are various practices to manage information security in organisations. The practices include the implementation of information security management systems (ISMS) in the organisations. Information security management systems emphasise the purpose to formalise responsibilities and control prescribed processes (David, 2002). In the next sections, a review of information security management systems found in the literature is demonstrated.

2.4.1 ISO/EIC 27001:2005 Standard

This is an international standard for information security based on British Standard BS 7799. The standard has adopted a process approach that establishes, implements, operates, monitors, reviews, maintains and improves an organisation's information security management system (ISMS) (BS, 2005). The standard implements the Plan-Do-Check-Act (PDCA) model to all its processes. "Plan" means execute the ISMS; "Do" means execute and manage the ISMS; "Check" means scrutinize and reassess the ISMS; and "Act" means preserve and enhance the ISMS (BSI, 2005). Compliance with ISO/IEC 27001:2005 guarantees that an organisation has achieved a certain level of compliance level for each of the eleven clauses addressed. The clauses covered are:

- "Information security policy"
- "Organisation of information security"
- "Asset management"
- "Physical and environmental security"
- "Human resources security"
- "Communications and operations management"
- "Access control"
- "Information systems acquisition, development and maintenance"
- "Information security incident management"
- "Business continuity management"
- "Compliance" (BSI, 2005, p.13-28)

2.4.2 ISO/IEC 27002:2005

This is an internationally accepted best practice for information security based on British Standard BS 7799-1. It is a code of practice for information security management (BSI, 2007). It provides guidelines for implementing the ISO/IEC 27001:2005 standard.

2.4.3 ISO/IEC 27005:2008

This is an internationally accepted standard for information security risk management. The standard defines a process to manage risk including establishing the context, assessment of risk, treatment of risk, acceptance of risk, communication of risk and monitoring and reviewing of risk (BSI, 2008). The process follows the PDCA model. In order to understand ISO/IEC 27005:2008 one has to be aware of ISO/IEC 27001 and ISO/IEC 27002 standards. According to Singh and Lilja (2009) the standard is unable to prioritize controls and to measure the impact of security enhancements.

2.4.4 NIST 800-14

It is a United States of America special publication on generally recognized standards and customs for security of information technology systems based on OECD's guidelines for information security (NIST, 1996). The publication elaborates eight standards to be met by information security program which are:

- To support the mission of the organisation
- To be a vital ingredient of robust administration
- To be financially sustainable
- To share security responsibilities to external users
- To make clear security responsibilities and accountability of users
- To use a comprehensive and integrated approach in design of security program
- To be reviewed regularly
- To consider social issues

Also, the publication elaborates fourteen customs to be met by information security program which are:

- Security policy
- Organisation of program
- Organisation of Risk
- Planning of security
- Employee/User factors
- Planning for incidents and disasters
- Information security incident management
- User education and awareness
- Computer security, support and operations

- Physical and environmental security
- Authenticity
- System access control
- Audit tracks
- Encryption

2.4.5 Control Objectives for Information and related Technology (COBIT)

It is a risk based IT governance framework developed by Information Systems Audit and Control Association (ISACA). It is based on the scrutiny and integration of existing IT standards and best practices (ITGI, 2007). According to ITGI (2007) the framework guarantees IT is aligned with the business; IT permits the business and maximises benefits; IT resources are utilized sensibly and IT risks are controlled properly. COBIT refers amongst many processes, to information security process. The COBIT framework enables administrators to bridge the gap between control requirements, technical challenges and operational risks.

2.4.6 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE is a risk base approach for managing information security that is inclusive, systematic, driven by the situation, and self directed. It was developed at Carnegie Mellon University. The approach is organised in three phases which are (i) build asset-based threat profile; (ii) identify infrastructure vulnerabilities; and (iii) develop security strategy and planning. The pillar of OCTAVE is structured interviews at various levels of an organisation to identify critical assets, risks on those assets, and design mitigation strategies for the assets (Alberts and Dorofee; 2003). OCTAVE approach employs PDCA cycle.

2.4.7 Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a United State of America federal law that provide protection on health information stored by organisations that handle personal health information. The act identifies a list of administrative, physical and technical guidelines for organisations to implement in order to ensure confidentiality, integrity, and availability of digital health data (HHS, 2012).

2.4.8 Holistic Security Management Framework (HSMF)

HSMF is a framework base on a holistic model to manage security of electronic commerce through efficient interaction among business process, security challenges of technology, and societal challenges of security (Zuccato, 2007).

2.4.9 Information Security Retrieval and Awareness (ISRA)

This is a holistic model for improving information security awareness on employees. The model is centred on social issues because they have always been overlooked (Kritzinger and Smith; 2008).

2.4.10 Open Web Application Security Project (OWASP)

OWASP is a non-profit organisation aimed at enhancing software security. Their "mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks" (OWASP, 2010). OWASP develops guidelines for testing software issues under free and open source license. The OWASP guidelines have explicitly defined known vulnerabilities and also the preventive measures that need to be taken (OWASP, 2010). OWASP made an important contribution in creating a secured Web application especially regarding the reduction of the number of security weaknesses especially for online university application (Sedek, et al., 2009).

2.4.11 Information Technology Infrastructure Library (ITIL)

This is a framework that provides best practices for information technology. It provides guidelines on managing IT security using Control, Plan, Implement, Evaluate and Maintain steps. ITIL can be adapted to the needs of an organisation. It is used in association with other best practices such as ISO/IEC 27002 (Arraj, 2010).

2.4.12 Discussion

Some of the above approaches for information security management are country or industry specific such as NIST 800-14 and HIPAA. According to Anttila and Kajava (2010) the PDCA model adopted in some of the standards is applied in the standards rather unsystematically, vaguely, and meagrely for the comprehensive aims of information security management. The major limitation of the COBIT framework is the reality that it does not offer continuous process improvement (Anthes, 2004). Standards and other recognized references for information security management underline the significance of senior executives' commitment to information security management

(Anttila, 2007). But, according to Anttila and Kajava (2010) senior executives of large and small companies are not interested in information security in their own management practices and do not understand their managing role for information security. Also, information security management puts emphasis on information security policy. However, there is no statistically significant relationship between the presence of information security policies and the incidence and severity of security breaches (Doherty and Fulford; 2005). According to Glaser (2009) there exists no security framework that encompasses cultural features and indeed NIST 800-14, ISO/IEC 27001 and ISO/IEC 27002 have neglected the role of culture in information security completely. Kritzinger and Smith (2008) argue that technical information security issues should not outshine the non-technical information security issues. Theoharidou *et al*. (2005) argue that information security is evolving into a new paradigm that requires a multi-disciplinary approach and Dlamini *et al.* (2009) concludes that new research endeavours are required that narrow the gaps between social and technical issues. Kritzinger and Smith (2008), Zuccato (2007) and Anderson (2007) models incorporated both technical and social issues but are either too focused on a particular industry sector or have not been grounded through proper theoretical investigation. Finally, information security standards and best practices provide guidance and framework for best practice but not solutions. They need to be tailored to the requirement of the organisation (Siponen, M. and Willison, R., 2009). Also, they need to be tailored for institutions in the developed countries. In Principle (5) of the OECD stresses the implementation of information security to cater the needs of a democratic society (OECD, 2011). However, in many developing countries democracy is in confusion or not in the same level as developed countries.

2.5 Information security strategies

It is important to provide a long-term plan or strategy for information security. Information security strategy is defined as:

> An art of deciding how best to utilise what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defence organisation's information infrastructure(s) against internal and external threats by offering confidentiality, integrity and availability at the expense of least efforts and costs while still effective. (Park and Ruighaver; 2008, p.27)

Two levels of information security strategies can be found in the literature namely organisational and national. A Strategy helps to organise security in an organisation. Bowen et al. (2006) suggest that information security strategy must be integrated into organisational strategy. It is important that an organisation achieves its objectives. It is important for information security strategy to be part of corporate governance. Corporate governance is the means by which an organisation is managed, and to what targets (Coyle, 2004). Organisational information security strategy helps to achieve the objectives of protecting assets in the organisation. "Information security is direct corporate governance responsibility and lies squarely on the shoulders of the Board of the company" (von Solms, 2001, p.217).

2.5.1 National Information Security Strategies

The United Nations World Summit on Information Society (WSIS) recommended a strategy for information security that was adapted by many countries. The strategy has policies for

- protection of critical information infrastructure
- promotion of a cyber security culture in the world
- encouragement of harmonisation of national laws and international laws and their enforcement
- defending spam
- creation of monitoring, cautioning and incident response facilities; national framework for information sharing
- privacy, digital information and customer protection

The Ministry of Information and Communication Technology of Mauritius in consultation with Pricewaterhouse Cooper of India developed Mauritius's national information security strategy based on WSIS recommendations. The strategy is aligned with the mission of national ICT policy which aims to "transform Mauritius into an information-secure society, which supports the development of a trustworthy and competitive information economy" (NISS, 2007, p.176). The main aim of the strategy is to establish confidence and security in the utilisation of ICT systems. The aim will be achieve through several objectives including adoption of information security standards and encouragement of secure electronic services. The strategy lack an objective of establishing a research organ that could be use to get insight into success of the measures outlined in the strategy.

The Japanese information security strategy is designed to protect Japan against large scale cyber attack (NISC, 2010). The strategy employs PDCA approach to implement security countermeasures dynamically. The strategy proposes policy of developing information security policy that adapted to changes in the information security environment. The strategy will establish a triadic policy that covers national security, disaster management and defend users. Among measures for protection of infrastructure, the strategy will ensure IPv6-related information security and benchmarking of cloud computing.

Zanzibar has no information security strategy at national level. Zanzibar's Ministry of Infrastructure and Communications developed a National ICT Policy in 2011. This policy is still in draft format. The policy lack in-depth strategy for information security. Issues of encryption, IPv6, and cultural issues influencing security has not been covered at all.

2.5.2 Organisational Information Security Strategies

A useful example concerning the research objectives is provided by the University of Tennessee's IT security strategy which has identified the Information Security Office (ISO), which is under the Vice President and Chief Financial Officer as the office with all responsibility of the information security program which includes:

- The development of a robust IT security strategy
- The development of IT security policies and embracing of best practices
- Supervision and regulatory compliance across the entire university
- Vulnerability assessment and countermeasures
- Crisis management
- Network and systems monitoring
- Forensic investigation
- Information security consulting
- Compliance to policy and best practices
- Awareness and training in information security
- Business continuity management

The scope of the strategy is the complete university. The university is responsible for safety of its information both digital and non-digital format. The strategy is guided by the principles of confidentiality, integrity, and availability in relation with information and information systems resources. The strategy implements principles of least privilege and defence-in-depth (UT, 2007). In least privilege approach, a user is given minimum access privileges as necessary to execute a specific function. A defence-in-depth approach

combines human, management and technology to initiate multiple levels of protection. ISO will ensure that all members of the university have a role in the creation, execution, and maintenance of the security plan. ISO will initiate and maintain IT security committees that will develop and review policies. Also, ISO will be responsible with all the issues of compliance, communication, and exceptions policies. One of the objectives of the University of Tennessee is to conduct a risk analysis consisting of vulnerability assessment and quantification of consequences of those risks (UT, 2007).

ICT security strategy for Western Cheshire NHS has several objectives for protection of their information assets. The strategy includes objectives on responsibility for confidentiality, integrity, and availability of the information assets controlled and maintained by the Cheshire ICT operations. The strategy will set a benchmark to be achieved by organisations and expect the collaborations and contribution of all executives and employees. The strategy will guarantee all sectors administered and maintained by the Cheshire ICT Operations comply with the strategy. The strategy adopts the obligations of the NHS Connecting for Health (CfH), Information Governance Toolkit, Code of Practice for Information Security, Healthcare Commission Standards and ISO/IEC 17799:2005 (NHS Western Cheshire, 2010). According to the strategy, a permanent Information Security Officer will be employed with responsibility of developing and executing an ICT Security Policy and its maintenance guidelines. In addition, an Information Security Officer will manage the communications and training programme of the strategy. Also, the Information Security Officer in association with an independent assessor will monitor the strategy for compliance. The strategy guarantees the continuity of operations in sustaining of clinical and production targets. The strategy outlines the development of policies and guidelines to be outsourced to Information Governance Group and Cheshire ICT Service business management team. Also, there will be periodic reviews of the strategy.

Brigham Young University strategy has objectives that are designed to provide protection according to clauses in ISO17799:2005 code of practice. Some of the measures that will be taken by Brigham Young University include encrypting classified information, establishing a VPN, conducting vulnerability assessment using NESSUS, encouraging the use of OWASP guidelines for web application, and not to allow anything from the Internet to have direct access to the university's network (BYU, 2008).

2.5.3 Discussion

The above strategies are unique to each organisation and nation. Each strategy has its own vision, aims, objectives, policies and measures to suit its environment. Each country or organisation has its own information security needs according to its features (Gerber and von Solms; 2005). Developing countries need to protect its information assets, but the type of technology they will implement will differ to those from developed countries. Strategies that are used in developed countries will not necessary work in the developing countries. The common policy among strategies presented above is benchmarking of information security practices.

2.6 Corporate governance

According to Coyle (2004) corporate governance is the method in which an organisation is managed, and to what aim. Also, corporate governance deals with practices and procedures that guarantee an organisation is run in a manner that enables it to reach its objectives (Coyle, 2004). "Corporate governance may be defined broadly as the study of power and influence over decision making within the corporation" (Aguilera and Jackson, 2010, p.487). According to Blair (1995), corporate governance includes the set of legislation, cultural, and institutional agreements that determine what publicly traded companies can do, who rule them, how power is executed, and how the risks and returns from the actions they assume are assigned.

A Board of Directors is obliged to effectively direct and control their institution as a whole (King Report, 2001; cited in Posthumus and von Solms, 2004, p.644). By directing and controlling an organisation they would, therefore, also govern information security (Entrust, 2004; cited in Posthumus and von Solms, 2004, p.644). In order to show management support to information security, executive management and the Board should develop an organisational information security policy (Whitman and Mattford, 2003; Corporate Governance Task Force, 2004; cited in Posthumus and von Solms, 2004, p.644). According to Fourie (2003) top management support is the most influential factor in information security management activities in an organisation. Top management are responsible for their organisation compliance to laws and regulations. It is vital for organisations to be able to evaluate their information security compliance level (Luthy and Forcht, 2006; Saleh, Alrabiah and Bakry, 2007). Top management are responsible to the risks facing their organisation. Analysis of information security risk presents organisations with increased awareness and more depth of understanding regarding their anticipated loss due to security breaches (Gerber, von Solms, and Overbeek, 2001).

2.7 Culture

Culture has been identified as an important factor of human behaviour. Culture is "a set of shared values and beliefs" (Javidan and House 2001, p.293). Beliefs are the perceptions of people on how thing are done in their nations. Values are aspirations of people about how things should be done. Also, Culture can be defined as "the collective programming of the mind which distinguishes the members of one human group from another" (Hofstede and Hofstede, p.4). The Global Leadership and Organisational Behaviour Effectiveness (GLOBE) Project defines culture as "shared motives, values, beliefs, identities, and interpretations or meanings of significant events that result from common experiences of members of collectives that are transmitted across generations" (House and Javidan, 2004, p.15). Culture can be categorised into different levels: national, organisational, regional, religious, gender, and group level. This thesis, will only deal with culture at national and organisational level. Organisations are influenced by the communities in which they are surrounded (Dickson et al, 2004).

2.7.1 National Culture

National culture is manifested mostly in values and less in practices while organisational culture resides mostly in practices and less in values (Hofstede, 1997). National culture can be measured empirically through dimensions of culture which are relative to other culture (Hofstede and Hofstede; 2005, p.4). Hofstede and Hofstede (2005) identify five dimensions of national culture: (1) Power distance is the extent to which power is dispersed among members of organisations within a country; (2) Uncertainty avoidance is the extent to which the culture feels endangered by unfamiliar happenings; (3) Individualism refers to the degree of importance of an individual's requirements compared with the group's needs as a whole; (4) Masculinity refers to the extent to which cultures show evidence of masculine or feminine qualities; and (5) Long-term orientation is the extent to which members of organisations promote behaviours inclined toward future gains. Hofstede (2010) added another dimension of national culture which is Indulgence. Indulgence is defined as "a tendency to allow relatively free gratification of basic and natural human desires related to enjoying life and having fun" (Hofstede, 2010, p. 281).

According to the GLOBE Project there are nine national culture dimensions (House et al, 2004). These dimensions are Power Distance, Uncertainty Avoidance, Humane

Orientation, Institutional Collectivism, In-Group Collectivism, Assertiveness, Gender Egalitarianism, Future Orientation, and Performance Orientation. These dimensions were derived empirically by the Globe Project. Moreover, the theoretical base that grounds the GLOBE project is integration of implicit leadership theory (Lord & Maher, 1991), value/belief theory of culture (Hofstede, 1980), implicit motivation theory (McClelland, 1985), and structural contingency theory of organizational form and the effectiveness (Donaldson, 1993; Hickson, et al, 1974). House et al (2004) define national culture dimensions as follow:

- Power Distance is the degree in which members of a society expect power to be shared equally.
- Uncertainty Avoidance is the degree to which society, organisation, or group depends on social norms, regulations, and processes to ease uncertainty of future events.
- Humane Orientation is the extent to which a society encourages and reward individuals for being fair, altruistic, generous, caring, and kind to others.
- Institutional Collectivism is the extent to which organisational or societal practices reward and promote sharing of resources and collective action.
- In-Group Collectivism is the extent to which people express pride, loyalty, and solidness in their organisations or families.
- Assertiveness is the extent to which people are assertive, confrontational, and aggressive in their relationships with others.
- Gender Egalitarianism is the extent to which a society reduces gender inequality.
- Future Orientation is the degree to which people engage in future-oriented behaviours such as delaying indulgence, planning, and investing in the future.
- Performance Orientation is the extent to which a society encourages and rewards members for performance advancement and brilliance.

This research adopts national culture dimensions proposed by the GLOBE Project because it covers much human behaviour through its nine dimensions. In addition, GLOBE Project integrates the theory of implicit motivation, theory of implicit leadership, theory of culture of value/belief, and theory of structural contingency of organization. By grounding many theories in GLOBE Project makes dimensions of much stronger.

2.7.2 Organisational Culture

Organisational culture describes how staff views the organisation. Schein (2004, p.17) has defined an organisational culture in term of a group culture as:

> A pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.

Also, Schein (2004) categorised organisational culture into three levels:

- Artifacts in organisations are (i) visible, (ii) tangible, and (iii) perceptible outcomes of activities grounded in values and perceptions. Artifacts include but not limited to dressing, communications and customs.
- Espouse beliefs and values in organisations are the social principles, philosophies, goals, standards and beliefs considered to have intrinsic worth for members of the organisation. Values include the beliefs held by members of the culture.
- Underlying Assumptions represent taken-for-granted beliefs about reality, feelings and human nature.

Hofstede and Hofstede (2005) described six dimensions of organisational culture which are:

- Process oriented, where members of the organisation circumvent risks and use minimum endeavour in their daily work.
- Employee oriented, where employees view that their organisation values them and vital decisions are made teams.
- Parochial, where staff gets their identity originated from the organisation.
- Open system, where members considered their organisation receives anyone.
- Loose control, an organisation where no strict in cost or work schedules and frequency of jokes is a norm.
- Normative, an organisation where compliance with organisation rule is more significant than outcomes.

According to Cameron and Quinn (2006) organisational culture dimensions are:

- Dominant Characteristics
- Organisational Leadership

- Management of Employees
- Organisation Glue
- Strategic Emphases
- Criteria of Success

These dimensions were empirically derived and result in four major types of organisational cultures which are Clan, Adhocracy, Market, and Hierarchy (Cameron and Quinn; 2006). The dimensions are grounded by Competing Values Framework (Quinn and Cameron; 1983) and relate to the effectiveness of an organisation. Cameron and Quinn (2006) developed Organizational Culture Assessment Instrument (OCAI) for measuring organisational culture. OCAI was used by over 10,000 companies worldwide (OCAI, 2010). Cameron and Quinn (2006) define the four cultures as:

A clan culture is:

> A very friendly place to work where people share a lot of themselves. It is like an extended family. The leaders, or head of the organization, are considered to be mentors and, maybe even, parent figures. The organization is held together by loyalty or tradition. Commitment is high. The organization emphasizes the long-term benefit of human resource development and attaches great importance to cohesion and morale. Success is defined in terms of sensitivity to customers and concern for people. The organization places a premium on teamwork, participation, and consensus. (Cameron and Quinn; 2006, p.66)

A hierarchy culture is:

> A very formalized and structured place to work. Procedures govern what people do. The leaders pride themselves on being good coordinators and organizers, who are efficiency-minded. Maintaining a smooth-running organization is most critical. Formal rules and policies hold the organization together. The long-term concern is on stability and performance with efficient, smooth operations. Success is defined in terms of dependable delivery, smooth scheduling, and low cost. The management of employees is concerned with secure employment and predictability. (Cameron and Quinn; 2006, p.66)

An adhocracy culture is:

> A dynamic, entrepreneurial, and creative place to work. People stick their necks out and take risks. The leaders are considered to be innovators and risk takers.

> The glue that holds the organization together is a commitment to experimentation and innovation. The emphasis is on being on the leading edge. The organization's long-term emphasis is on growth and acquiring new resources. Success means gaining unique and new products to services. Being a product or service leader is important. The organization encourages individual initiative and freedom.
>
> (Cameron and Quinn; 2006, p.66)

A market culture is:

> A results-oriented organization. The major concern is getting the job done. People are competitive and goal-oriented. The leaders are hard drivers, producers, and competitors. They are tough and demanding. The glue that holds the organization together is an emphasis on winning. Reputation and success are common concerns. The long-term focus is on competitive actions and achievement of measurable goals and targets. Success is defined in terms of market share and penetration. Competitive pricing and market leadership are important. The organizational style is hard-driving competitiveness.
>
> (Cameron and Quinn; 2006, p.66)

Dominant characteristics are the features that employees view their organisation to be such as organisation to be a personal place, a place where employees share things, an entrepreneurial place, and a place where employees can take a risk among others (Cameron and Quinn; 2006).

The organisational leadership dimension involves the features of leadership in the organisation as viewed by employees. These features include but are not limited to mentoring or nurturing, entrepreneurial or innovation, no-non-sense or aggressive, and coordinating or smooth-running (Cameron and Quinn; 2006).

The management of employees dimension has features that employees view their organisation to have such as teamwork, freedom, high demands, and security of employment among others (Cameron and Quinn; 2006).

Organisational glue dimension have features that employees view their organisation are glued upon such as loyalty and mutual trust; innovation and development; emphasis on achievement, and formal rules and policies (Cameron and Quinn; 2006).

The strategic emphasis dimension includes features such as human development, acquiring new resources, hitting stretch targets, and permanence and stability among others (Cameron and Quinn; 2006).

The criteria for success dimension has features such as teamwork, product leader or innovator; outpacing the competition and low-cost production (Cameron and Quinn; 2006).

In the GLOBE Project, dimensions of organisational culture and national culture are analogous. Handy (1995) categorised organisation culture into four cultures:

- Club culture describes organisations that have a division of task based on purposes and merchandises.
- Role culture describes organisations where its approach is inclined towards defining role or task to be accomplished.
- Task culture describes organisations where administrators are involved with constant and thriving resolution of a crisis.
- Existential culture described organisations that operate on assumptions that they support the individuals of those organisations to do their own stuff.

This thesis adopts organisational culture based on Cameron and Quinn (2006) because the dimensions of culture were grounded by Competing Values Framework that relates to the effectiveness of an organisation. Many organisations in Zanzibar are not effective in their operations. Many of the organisations are run on public finance or family investment. Competing Values Framework is not based on national culture behaviours but more on organisational business attitude.

2.7.3 Information Security Culture

Schlienger and Teufel (2002) define information security culture as "all socio-cultural measures that support technical activity methods, so that information security becomes a natural aspect in the daily activity of every employee". While Dhillon (1995) defines security culture as "the totality of human attributes such as behaviours, attitudes, and values that contribute to the protection of all kinds of information in a given organisation". And, Ngo et al (2005) terms information security culture as "how things are done (i.e. accepted behaviour and actions) by employees and the organisation as a whole, in relation to information security". Several studies found in the literature investigated information security culture in organisations. Chaula et al (2006) investigated information security culture in a commercial public organisation. Some studies focus their investigation on the

culture of organisation, and concluded that organisations must stress the idea that information security is the responsibility of every member (Schlienger and Teufel, 2002; Vroom and von Solms, 2004). Chaula et al (2006) based their study on GLOBE project while Schlienger and Teufel (2002) based their study on Schein (2004).

2.7.4 Discussion

National culture influences the adoption of innovations (van Everdingen and Waarts; 2003) and how people in certain societies view their responsibilities, interact and convey their feelings (Hofstede, 2001). Many developing countries have imported information systems innovation from developed countries. Importation of information systems forces developing countries to adopt ideas that are not appropriate to their local context (Bhatnagar, 2000; Albirini, 2006).

Hall (1976) finds that in low context cultures, most of the information is contained in the message itself in an explicit and detailed way. On the other hand, in high context culture, less explicit and detailed information is carried in the message itself and inferences are drawn from implicit information. It is accepted that communication is an important facet of information security management (von Solms and von Solms, 2004b; Hone and Eloff, 2002) and effective communication between IT, management and users is challenging enough to achieve in organisations even though the culture is relatively homogeneous. Consequently, in high context cultures, communication tends to be a key issue related to information security.

Hofstede studies are based on investigation on employees from IBM Corporation. GLOBE Project investigated culture by using managers as participants. These two types of participants could have influenced the results. IBM's employees are involved with technology and would have good education. Educated people have different culture to common people. The same is true for managers who are among the best educated in the society. It is important that we have empirical data that reflect the culture in the context of Zanzibar. The empirical data that reflect Zanzibar culture will be collected by conducting an investigation of employees of organisations in Zanzibar.

2.8 Organisational semiotics

Semiotics is the "science of signs". A sign represents something to someone. All types of signs are involved in semiotics including oral language, images, literature, videos, sound, body language, plays and texts among others. Semiotics is involved with the life cycle of a sign from being produced, through being processed, to its usage, with stress on the

impact of signs (Liu, 2000). All signs have meaning (semantics), relationship among signs (syntactic), and usage (pragmatics). In the study by Stamper (1973) noted that there are three more features of signs: physics, empirics, and social world. These six features of signs collectively are called semiotic ladder or semiotic framework (Liu, 2000).

Organisational semiotics is the study of organisation using sign systems as communication tools between human beings, information, and technology within a social reality (Liu, 2000). "Organisational semiotics defines an organisation as a social system or a social structure in which people behave in an organised manner by conforming to a certain system of social norms" (Rambo, Liu and Nakata; 2009). Norms make members of an organisation behave, think, judge, and view the world (Stamper et al., 2000). Culture or subculture is made up of shared norms. Norms and signs always go together. Therefore, culture or subculture could be represented by all kind of signs. According to Gottdiener (1995), a sign is composed of expression and content. Signs are tools that facilitate social interactions (Gottdiener, 1995). A sign is a medium for human to understand things. People communicate significance, create meanings, and convey thoughts and sentiments via signs or sign systems. Signs and norms cannot be separate (Stamper, et al., 2000).

Organisational semiotics can be used to analyse and develop organisations, economic transactions and information systems through the use of approaches, models and procedures that have been designed as substitutes to conventional approaches (Gazendam, 2004). Several studies have adapted a semiotics approach to analysing various challenges related to information systems. Li et al (2008) used organisational semiotics to develop a personalised clinical pathway. French et al (2006) developed e-Service Trust framework based on a semiotic framework. Andersen (2001) argued about the function of semiotics in the creation of a user interface and declared that semiotics is useful for arranging the design of information systems in a wider theoretical and philosophical framework. Liu (2002) discussed that as an outcome of the failure of users to recognize the meanings of words and the failure of designers to appreciate user requirements, an approach with an emphasis on semantics is required to explain meanings to enhance communication channels. Sjostrom and Goldkuhl (2003) demonstrated a socio-pragmatic and semiotic concept of user interfaces and discusses that conceptualising user interfaces by using the semiotic paradigm makes way for understanding IS exploit as social action and understanding how IS artefacts can be viewed as communicative tools in such social exploit. Also, Dhillon and May (2006) used semiotics to structure an improved

understanding of information security in the framework of human computer interaction (HCI).

2.9 Non-profit organisations

There are several definitions for a non-profit organisation. A non-profit organisation is also referred as a not-for-profit organisation. The International Classification of Non-profit Organisations (ICNPO) defines a non-profit organisation as the organisations with the following features (Salamon and Anheier, 1996):

- "Organized, i.e., institutionalized to some extent" (p.2)
- "Private, i.e., institutionally separate from government" (p.2)
- "Self-governing, i.e., equipped to control their own activities." (p.2)
- "Non-profit-distributing, i.e., not returning profits generated to their owners or directors." (p.3)
- "Voluntary, i.e., involving some meaningful degree of voluntary participation." (p.3)

Some studies have categorised a non-profit organisation in terms of a non-governmental organisation (NGO). NGO is included in the UN Charter (Martens, 2002). The essential defining element of a non-profit organisation is the prohibition to distribute profits in which Lyons and Hocking (2000) term as the "non-distribution clause". This research project adopts the definition of non-profit or not-for-profit organisation developed by the Association of Chartered Certified Accountants (ACCA). According to the ACCA (2012) non-profit or not-for-profit organisation have the following characteristics:

- "Do not have external shareholders providing risk capital for the business"
- "Do not distribute dividends, so any profit (or surplus) that is generated is retained by the business as a further source of capital"
- "Their objectives usually include some social, cultural, philanthropic, welfare or environmental dimension, which in their absence, would not be readily provided efficiently through the workings of the market system"

With the above characteristics, some public organisations are non-profit organisations. Public organisations that provide services such as identity cards production, health services, and education are good examples of non-profit organisations. The solutions mentioned in section 2.4 are expensive, complex, need skilled personnel to implement

and were designed to cater for large commercial organisations (Simmons and Burgess, 2000; Brake, 2003, cited in Dimopoulos et al, 2004).

2.10 The case study (Zanzibar)

Zanzibar is an archipelago consisting of two major Islands of Zanzibar and Pemba. It is a semi-autonomous part of the United Republic of Tanzania but has its own Government and is led by its own President. The House of Representatives is responsible for passing new laws in Zanzibar. Members of the House of Representatives come from two major political parties. Figure 2.10.1 shows the map of Zanzibar. The population of Zanzibar is 1,211,000 (OCGS, 2011). The vast majority of Zanzibaris are Muslims. Although a large population of the Zanzibar people are Muslims, the government of Zanzibar is ruled by secular laws. Ethnic groups in Zanzibar are Africans, Indians, Arabs and Europeans. The national culture of Zanzibar is based on the Swahili culture which is a mix of ethnic groups (Vander biesen, 2009). In the study by Hofstede (2010), Zanzibar's national culture dimensions are in the category of Tanzania or East Africa. Table 2.10.1 shows Zanzibar's national culture dimensions.

Figure 2.10.1 – Map of Zanzibar (Source: MAPAS (2012))

Table 2.10.1 shows that Zanzibar society has inequality in sharing of power; favours group's needs; believes in masculinity qualities; moderation in dealing with unexpected events; and not inclined to the future. The public sector forms 3.4% of the Zanzibar population (OCGS, 2011). The Zanzibar public sector provides services such as education, health, transportation, power, finance, communications, agriculture, legislation and social services. In addition, Zanzibar's Gross Domestic Product per capita is US$561 (POFEDP, 2012). The Government of Zanzibar has adopted various information systems to facilitate the way services are offered to its citizens and improve efficiency in work places. Information systems that were adopted include, but are not limited to, the integrated financial system, payroll systems, human resources systems, the driving licensing system, the road licensing system, tax systems, the Value Added Tax (VAT) system, the car registration system, the registration of death and birth system, the citizen registration system, voter registration and various websites that offer information about various issues and forms for online and offline filling. This adoption is part of a long term development strategy called Zanzibar Development Vision 2020 to be achieved by the year 2020. In 2012 Zanzibar planned to adopt the e-government system (Sultan, 2011). Marine fibre optic cable will arrive in Zanzibar in 2013 that will carry high-speed broadband. The population of United Republic of Tanzania is 43,188,000 (NBS, 2010). Table 2.10.1 shows number of internet users increased between 2008 and 2010. Table 2.10.2 shows massive gap between Tanzania and USA in the usage of computer and internet.

Table 2.10.1: Zanzibar's national culture dimensions (Source: Hofstede (2010))

Culture Dimension Index	**Zanzibar (Tanzania or East Africa)**	**Saudi Arabia or Arab Countries**	**Great Britain**
Long-term orientation (LTO)	34	36	51
Power Distance (PDI)	64	80	35
Individualism (IDV)	27	38	89
Masculinity (MAS)	41	53	66
Uncertainty Avoidance (UAI)	52	68	35

Table 2.10.2 – Internet Usage in Tanzania (Source: TCRA (2010))

Access type	**2008**	**2009**	**2010**
Internet Cafe	126,000	215,640	260,280
Organisation/Institution	2,444,000	2,588,000	2,663,200
Household/Individual	993,732	1,574,752	1,932, 816
TOTAL	3,563, 732	4,378,392	4,856,296

Table 2.10.3 – Computer and Internet usage in 2007 (Source: ITU, 2009)

Country	% of household with computer	% of household with internet
Tanzania	2.3	0.6
USA	70	62

Zanzibar was ruled by Oman Arabs in 19 century as a Sultanate of Zanzibar. Then, Sultanate of Zanzibar was provided protection by the British and became Zanzibar British Protectorate. In 1963, it became independent from the British. In 1964, there was a revolution that led to the formation of the current Government. Although Zanzibar is a democratic country, all the elections are marred by violence. Members of Civil United Front (CUF) who are the main opposition party in Zanzibar believe that they are oppressed by the Government of Zanzibar (Brent and Mshigeni; 2004). According to Brent and Mshigeni (2004) CUF has formed youth wings called Blue Guard and White Guard as party's security arm. Sadallah (2010) reported that the CUF Presidential candidate in Zanzibar has suspicion on vote rigging at the headquarters of the ruling party using electronic means.

2.11 Rationale for the focus on information security in non-profit organisations

This thesis is focused on improving the governance of information security in Zanzibar's non-profit sector. The non-profit organisations make crucial contributions to economic, social and political aspects of Zanzibar's life. Indeed, the non-profit sector is the major employer in Zanzibar. The non-profit organisations provide vital services to the community including health, education, law enforcement, environmental protection, voting, citizen's registry, social welfare, public finance, and human rights. Employees of non-profit organisations in Zanzibar often have a relaxed attitude in doing their daily tasks because of lack of fear of losing the jobs; services in these organisations are delayed

due to employees' attitudes toward work. The non-profit sector in Zanzibar depends mostly on lowly paid public sector employees and volunteers to be run. This makes the non-profit organisations to have low skilled IT workers.

The practices of information security governance in non-profit organisations have much influence not only within the organisations themselves. Many of the non-profit organisations have computers that are connected to the Internet. Many of the non-profit organisations depend on email services provided by free web-based email services such as Yahoo and Hotmail. Confidential information could be passed through untrusted networks via emails. Computers connected to the internet can be attacked through vulnerabilities in operating systems and application software. Automated attacks can be launched remotely to create distributed denial of service attacks, or send a large amount of spam that could cripple the network. The distributed denials of service attacks are potentially threatening the practicability of the Internet (Sturgeon, 2007).

The major obstacle of non-profit organisations in contrast to commercial organisations is the lack of resources. This lack of resources is evidently found in the level of maturity of information systems in these organisations. The non-profit organisations have smaller budgets for IT programmes and smaller personnel dedicated to IT department. The lack of resources and technological skills in non-profit organisations make them "fall even further behind in their quest to support and improve their programs" (Schneider 2003, p.383). Hackler and Saxton (2007) find that "the capacity of a non-profit to enlist new technologies to deliver services in new ways (e.g., online commerce and databases) is missing, and this is the step that would allow nonprofits to embrace IT innovation" and Nielsen (2012) added that "a non-profit organization in a developing country cannot afford to fail to implement an information system, but this can often be the case because of little expertise on the area". New information systems emerge every day, which make it difficult for non-profit organisations to make informed decisions on what security measures to implement in their organisation. Also, training employees every time when new systems are installed put too much pressure on managers on allocating the few resources the organisations have to training schemes.

The size of a non-profit organisation in most cases tends to be smaller. Some studies indicate that the larger the organisation the more likely for them to have implemented an information security governance system (Hong, Chi, Chao, and Tang, 2006; Chang and Ho, 2006). This implies that the smaller the organisation the more likely it is not to have implemented an information security management system. Also, the industrial sector of

the organisation is a determining feature in the establishment of an information security management system, for example, the banking sector gives a high priority on information security governance (Chang and Ho, 2006; Hong et al., 2006). Consequently, the Payment Card Industry (PCI) Data Security Standard (DSS) was established to provide protection for cardholder data security worldwide. The USA has a huge profitable healthcare industry; therefore HIPAA is a standard that was established to protect personal health information in the USA. Research indicates that smaller organisations have the following characteristics:

- Employees find security solutions to be complex and confusing (Blake, 2003)
- Information security is not a priority (Yildirim et al., 2011)
- Perceiving that they are not the target of hackers and cyber criminals and only need protection from virus
- Dependence of vendors and consultants for awareness and skills (Suppiah-Sandre, 2002)
- Working in a sector that accept risk (Lacey and James, 2010)

As mentioned earlier, the importance of the non-profit sector in Zanzibar for socio-economic and political aspects make it vulnerable to insider threats. According to CERT (2010) insider threat remains one of the most expensive threats. Human error constitutes for a significant cause of information security threats and often undervalued during the risk assessment (Im and Baskerville, 2005). Low pay in Zanzibar's non-profit sector makes them more vulnerable to such risk.

The academic literature for information security practices in non-profit organisation is tremendously rare especially for developing countries. For this reason and in view of the above discussions the focus of this thesis on enhancing information security governance is on non-profit organisations.

2.12 Conclusion

The objective of this review is to look at the area of information security, information security management, information security in the developing countries, culture, organisational semiotics, Zanzibar and concepts and challenges related to information security management. The existing literature was analysed with the aim of gathering information on diverse features of information security management. The analysis has revealed that information security is one of the main values in the success of any organisation. Organisations are influenced by the culture they are surrounded. An

organisation must have long term strategy for information security. Existing strategies are country or industry specific and need to be tailored to suit the environment that the organisation resides. The literature revealed that social issues are as important as technical issues in managing information security. The analysis has identified organisational semiotics as a model that could analyse and integrate social and technical issues.

The literature review in Section 2.3 revealed that there is a problem of information security in the developing countries. The literature review in Section 2.10 exposed that Zanzibar which is a developing country is in the process of adopting various information systems in its organisations. But, the review shows that Zanzibar is facing many social, economical and political challenges. The literature review in Section 2.5 demonstrated that information security strategies are unique to each country and organisation according to their needs and feature. This led the researcher into asking the main research question RQM which is "*What are organisational factors need to be tackled or managed to develop and implement effective information security governance in the context of Zanzibar?"*

The literature review in Section 2.4 and 2.5 revealed that there are several information security management systems and strategies. The review shows that these strategies and systems are not perfect, which means should not to be adopted as they are. There are many gaps in existing information security management systems and strategies. PDCA model adopted by some standards is applied erratically in the model. COBIT framework does not offer continuous process improvement. Senior managers in organisations are not interested in information security or do not understand their managing role for information security. There is no significant correlation between having an information security policy and occurrence and severity of security violations. The literature showed that information security policy is the backbone of information security management systems. The literature review in Section 2.5 disclosed that there are many different types of strategies with unique missions and visions. It is important to critical analyse these different types of strategies. This led to the research question RQ1.

The literature in Section 2.2 revealed that there are so many threats that organisation may face such as social engineering, automated attacks, insider threats, phishing, spyware, spam, virus among others. The literature review in Section 2.9 revealed that non-profit organisations are important in Zanzibar for its contribution in social, economical and political aspects. The literature in information security for non-profit organisation in the

developing countries is rare. Information systems in non-profit organisations lack maturity. Information security standards and best practices were designed for large commercial organisations in developed countries. Many non-profit organisations are small and do not feel that information security is important to them. It has been revealed that non-profit organisation could be a target of a distributed denial of service attack that will spread to other organisations. This led the research to the research question RQ2. The literature review in Section 2.4 shows that ISO/IEC 27002 is a process based implements the PDCA model. Also, ISO/IEC 27002 is an international accepted best practice in information security that provides guidelines for implementing ISO/IEC 27001 standard. Section 2.4 demonstrated that ISO/IEC 27005 is an international accepted standard for information security risk management that implement PDCA model. The OCTAVE approach is a huge and complex method to digest for smaller organisations. The COBIT framework does not offer process improvement.

The literature review in Section 2.10 revealed that Zanzibar is a country with multi-ethnic groups. Zanzibar faces social, economical and political challenges. The literature review in Section 2.4 demonstrates that information security management is becoming a multi-disciplinary approach and new research endeavours are required to integrate social and technical challenges. In addition, existing security standards and best practices have not encompassed cultural features. The literature in Section 2.7 revealed that there are many dimensions of culture. There is a lack of research in culture specific for Zanzibar. The existing studies show that culture of Zanzibar has been included as part of East Africa (Hofstede, 2010) or Tanzania GLOBE study (House et al., 2004). This led to the research question RQ3.

The research question RQ4 was asked in order to achieve the research aim (RQM, Section 1.1). Research questions RQ1, RQ2 and RQ3 will provide the answer for the research question RQ4. The research RQ1 will identify the gaps for the rationale of developing a new framework for information security culture. The research question RQ2 will provide empirical data for information security practices the organisations. The research question RQ3 will provide empirical data for the cultural behaviour in the study environment.

The next chapter, Chapter 3, presents a description of methodological selections employed in this research project.

CHAPTER 3

3 RESEARCH METHODOLOGY

3.1 Introduction

In the previous chapter, the literature that is used to build the theoretical foundation of this research was discussed. In this chapter, the research approaches that were considered to address the research questions identified in the Chapter 1, the criteria to identify their relevance for the project and the reasoning behind their choice will be investigated. This chapter describes the approach that will be used to answer the research questions and practical details for how the strategy is to be implemented in practice. The chapter will begin with a theoretical perspective of research approaches used in this project. Then data gathering procedures are outlined. Finally, a data analysis plan and procedure are discussed, followed by a discussion of the validity and reliability of data for the research questions.

As discussed in Chapter 1 the main research question that needs investigation for this project is "to find organisational factors that can be tackled or managed to develop and implement effective information security governance in the context of Zanzibar". The nature of the question here can be best studied through a holistic approach. According to Iivari and Hirschheim (1996) a social-technical approach is a vital strategy for addressing organisational and social challenges. The mixed methods approach, involving integration of qualitative and quantitative data, presents a broad understanding of the research question (Creswell, 2009). A case study is an example of qualitative research. The use of a case study here will enable us to generalise the results for that case. The case in this study is non-profit organisations in Zanzibar. Due to lack of research in information security in the Zanzibar context, an interpretive research approach is justified for this project. According to Kaplan and Maxwell (1994) an interpretive research approach helps

to understand a fact from the outlook of the participants and its particular social and organisational context. The interpretive research methods have been discussed to be useful in information systems research (Nelson, 2004; Walsham, 1993). Interpretive method forms the philosophical foundation of a qualitative research approach.

3.2 Research design

This study is steered by a philosophical assumption of interpretive epistemology. Epistemology is "the theory of knowledge, especially with regard to its methods, validity, and scope, and the distinction between justified belief and opinion" (OD, 2011). The epistemological assumption of the interpretive investigator is "findings are literally created as the investigation proceeds" (Guba and Lincoln, 1994, p. 111). Also, they clearly identify "understanding social reality requires understanding how practices and meanings are formed and informed by the language and tacit norms shared by humans working towards some shared goal" (Orlikowski and Baroudi, 1991, p. 14). Data collection and analysis were informed by qualitative and quantitative approaches. Figure 1.5.1 on Section 1.5 illustrates the overall research design. As stated in Section 1.1, the main research question in the thesis is: "what organisational factors need to be tackled or managed to develop and implement effective information security governance in the context of Zanzibar?" In the following sections, it is argued that the research design, by implementing an interpretive approach, was the most effective method to answer the research question.

3.3 Research approaches

"Research is one of the ways to find answers to your questions" (Kumar, 2005, p.6). In this project qualitative, quantitative and case study approaches are judged suitable to perform the research. The reason for this is the research has to be completed within a small time frame of three years. The quantitative methods will enable to gather data from a large sample much quicker. The research will investigate information security through observation of users and their surroundings; and analysed documents. This can be done through qualitative methods. Also, qualitative approach can provide quality data from smaller sample. The case study approach will enable the researcher to gather data from a natural setting of the sample. Case study can be implemented either quantitative or qualitative approaches or any mix of both (Doolin, 1996; Stake, 1994; Yin, 2003). I think the mix of both qualitative and quantitative approaches is the best method to understand a case study.

3.3.1 Quantitative approach

In the approach investigation is carried out systematically based on figures and statistical data. The investigators are not part of the research, they are the outsiders. According to Kumar (2005), a quantitative approach is structured and stresses on some kind of measurement, such as measurement of changes in phenomenon, situation, issue etc. Statistics may be used to increase confidence in presenting findings and influence of various variables in a quantitative study (Kumar, 2005). Examples of data collection methods for quantitative approaches are surveys and experiments (Creswells, 1994).

There are two types of experiments: 1) True experiment is when participants are selected randomly. 2) Quasi experiment is when participants are not selected randomly (Creswells, 1994). Random selection provides equal opportunity to participants in becoming involved with the experiment. Surveys are used to collect data by asking respondents about their experiences, attitudes, or knowledge. Data collection in a survey is done through questionnaires or structured interviews. Graziano and Raulin (2007) mentioned two types of surveys: 1) A status survey which explains the present features of a sample 2) A research survey which seeks present features of a sample and relationships among variables. Voter choices or employee satisfaction is an example of status survey. A survey on people's culture and its impact on security is an example of survey research.

Surveys are applied to describe the behaviour of a narrow or wider population (Heiman, 1998). The outcome of a survey on a sample can be generalised to the whole population (Fink, 2002). The outcome will be more accurate if the sample is larger. Also, unbiased sampling will increase the accuracy of the outcome. Use of questionnaires in surveys allows data collection from a wider population in short duration with less cost administering them to participants. With the questionnaires, one of the rationales is the respondents are free to answer the questions without being influenced by the researcher (Heiman, 1998). Interviews allow a survey to be performed quicker and extra information may be obtained from respondents, but the researcher might influence the response. According to Graziano and Raulin (2007) there are two types of survey designs: 1) Cross-sectional design is a survey which is conducted one time to a sample, resulting data on the measured features as they present at the point of the survey 2) Longitudinal survey designs is a survey which can be repeated to the same subjects at different times. In this thesis, cross-sectional survey is employed. The main reason for this is the time limitation to complete the research and financial constraint faced by the researcher. Also, the cross-

sectional survey designs enable to compare the performance of each organisation in the study at the same time and no interference with the participants in the research.

A questionnaire is a list of questions written in a paper or other media where respondents record their answers. Advantages of using questionnaires:

- Questionnaires allow anonymity of the participants.
- Questionnaires can be mailed to respondents.
- A researcher may administer questionnaires to a group of people gathered in one location.
- A website can be used as a questionnaire.
- A questionnaire can be self-administered in which respondents read the instructions and write the answers or choose their answers to the questions.

Questions in the questionnaires are closed-ended or open-ended. In the closed-ended questions, the respondents are given several options to select the best option for the answer. In the open-ended questions, the respondents write down the answer in their own words. Closed-ended questions are quicker to answer and analyse than open-ended questions. More information is gathered through open-ended questions because respondents are free to write their own thoughts and feelings. The responses will be examined carefully to generate the patterns and trends. Categories of different themes that emerge will be developed. Coding categories can be used to separate the material bearing on the subject from the data.

Interviews are another method of gathering information in the surveys. A structured interview is the interview in which questions are predetermined by the investigator using the same questions in the same order as determined in the schedule of the interview (Kumar, 2005). An interview can be done through the phone or face-to-face. A phone interview is expensive. Interviews are good for gathering in-depth information on challenging issues. Interviews consume a lot of time and investigators may influence the response. A structured interview represents a quantitative approach.

In this thesis, a quantitative approach was used for data collection because of the need to gather data from a large sample in a short time. Quasi experiment was used because of respondents were few due to their specific skills required which is user of computers, IT workers or managers. The survey used to gather data was the cross-sectional survey because of time and financial constraints, and the need to compare the performance of

organisations participated in the study. Questionnaires were used with closed-ended questions to make data collection process quicker. The questionnaires were distributed personal by the researcher and were self-administered by the respondents. Also, a structured interview was used to gather data faster. The interview was conducted face-to-face by the researcher because of financial constraint.

3.3.2 Qualitative approach

A qualitative approach is unstructured and allows flexibility in exploring the nature of a problem or phenomenon (Kumar, 2005). According to Kumar (2005) a qualitative approach has a smaller number of participants and can investigate their experiences, meanings and views of a problem under the investigation. Investigators interact with the participants in the study. "This means that qualitative researchers study things in their natural settings, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them" (Denzin and Lincoln; 2000, p. 3).

There are several types of qualitative approach found in the literature such as a case study, ethnography, grounded theory, phenomenological study, and action research (Creswell, 1994; Tierney, 1996; Parry, 1998). The approach used in this thesis is based on case studies. Data collection in qualitative approaches is interviews, observations, documents and audio visual materials (Creswell, 1994). This approach is beneficial where an in-depth understanding of a phenomenon is needed that means to answer the question in a bigger picture. In addition, qualitative methods provide the answer to why question and suitable for smaller population of respondents.

Interviews can be unstructured or semi-structured. Unstructured interviews allow flexibility in the questions. The questions are asked as more issues appear in the context of the interview. Semi-structured interviews have both predetermined questions and flexible questions that appear as more issues are uncovered.

Observation is a way in which a researcher watches and listens to dealing or phenomenon as it happens. Participant observation is when an investigator, involved in the tasks of the group being monitored in a similar approach as its members (Kumar, 2005). Non-participant observation is when an investigator, does not participate in the tasks of the group but remains an inactive witness, watching and listening to its tasks and making summarisation from this (Kumar, 2005). Observation can be recorded through narrative, scales, categorical recording or mechanically (Kumar, 2005). In this thesis, narrative will be used in recording the observations. According to Kumar (2005) narrative recording

involving “the researcher records a description of interaction in his/her own words” (p.121). Narrative is cheaper and simple to implement.

“Documents are standardized artifacts, in so far as they typically occur in particular formats: as notes, case reports, contracts, drafts, death certificates, remarks, diaries, statistics, annual reports, certificates, judgements, letters or expert opinions” (Wolff, 2004, p.284). Creswell (1994) added newspapers, meetings’ minutes, and private journals or diary as documents for data collection. Audiovisual items for data collections are computer programs, still images, videotapes, movie and art materials (Creswell, 1994).

3.3.3 Case studies approach

A case study is “an attempt to understand a person, institution, etc from collected information” (Allen, 1991, p.173). Oxford Dictionaries defines a case study as “a process or record of research into the development of a particular person, group, or situation over a period of time” (OD, 2011). Case studies inspect a phenomenon in its natural setting; utilizing multiple approaches of data collection to collect information from one or a few sources; and there are no clear boundaries between phenomenon and circumstance (Yin, 2003; Benbasat et al, 1987). In the literature case study approach has been used in answering “how” and “why” questions; or if researcher cannot manipulate the behaviour of participants in the study (Yin, 2003).

There are several types of case studies found in the literature including intrinsic, exploratory, explanatory, descriptive, multiple-case studies, instrumental and collective (Yin, 2003; Stake, 1995). The unit of analysis in a case study could be an individual, a community, an organisation, a nation-state or a phenomenon (Yin, 2003; Stake, 1995). The unit of analysis in this thesis is non-profit organisations in a developing country. This thesis will cover exploratory case study. Exploratory case study aims to explore those situations in which the intervention being evaluated has no clear, single set of outcomes (Yin, 2003). The lack of research in information security in the context of Zanzibar rationalises a selection of exploratory case study for this thesis hence this is why this type of approach is most relevant.

3.3.4 Interpretive research

According to Klein and Myers (1999), the underpinning theory for interpretive research is that knowledge is expanded, or at least sieved, through societal creations such as speech, consciousness, and shared significances. As far as methodology is concerned, interpretive research does not initiate dependent or independent variables, does not embark to

examine hypotheses, but intends to generate an understanding of the social perspective of the phenomenon and the process whereby the phenomenon influences and is influenced by the social environment (Walsham, 1995b). In qualitative and interpretive case studies, the researcher is directly engaged in the process of data gathering and analysis (Creswell, 1998; Klein and Myers, 1999; Morgan and Smircich, 1980; Morse, 1994); however, in the latter, the investigator, through close contacts with the subjects, becomes a "passionate participant" (Guba and Lincoln, 1994, p.115). It offers an opportunity to gain a great insight into the issue under investigation because "[a]n interpretive explanation documents the [participant's] point of view and translates it into a form that is intelligible to readers" (Neuman, 1997, p. 72). Certainly, interpretive research allows the possibility of presenting the researcher's own creations as well as those of all the participants (Guba and Lincoln, 1994; Neuman; Walsham, 1995a). The ontological assumption of the interpretive researcher is that societal realism is locally and exclusively created (Guba and Lincoln; 1994) "by humans through their action and interaction" (Orlikowski and Baroudi, 1991, p. 14). According to Walsham (1993) the purpose of interpretive research in information systems is to provide an awareness of the context of the information system, and the process whereby the information system manipulates or is manipulated by the context.

In this research, there was no examination of hypotheses, and any initiation of dependent or independent variables. The intention of the research is to understand cultural factors that impact the management of information security. Zanzibar has a population of people immigrated from different parts of the world, with different culture and ethnicity. The researcher was directly involved in the process of data collection and analysis. Also, the researcher was in close contact with the respondents. The researcher did develop the framework of information security culture with the help of the participants. This justifies the selection of the interpretive case study for this thesis.

3.4 Data collection

Data was collected through questionnaires, structured interviews, semi-structured interviews from members of organisations; through site observations and from organisational documents, and public documents. There were two phases of data collection in this study. Phase I involved data collection for investigating the state of information security in Zanzibar. The Phase II of data collection investigated complex societal issues that impact information security governance in the context of Zanzibar. Questionnaires gathered quantitative data; interviews, document reviews and site

observations gathered qualitative data. The findings of Phase I determined the extension of the research to Phase II. Phase I of the research was conducted between the end of February and the middle of March 2011. Phase II of the research was conducted between the end of April and the end of June 2012. Participants were allowed five working days to complete the questionnaires. Interviews were conducted between 7.30am and 3.30pm which are the official working hours in Zanzibar public sector. All the questionnaires used in this research are found in Appendix A. Table 3.4.1 presents the summary of the research approaches and instruments used in the research based on the four research questions which are:

RQ1. What are the existing information security strategies?

RQ2. What is the current state of information security governance in non-profit organisations in the context of Zanzibar?

RQ3. What are the cultural factors that impact upon information security governance in non-profit organisations in the context of Zanzibar?

RQ4. How can non-profit organisations improve their information security governance?

Table 3.4.1: Summary of the research approaches and instruments used

Research Questions	Research Approaches and Instruments							
	Quantitative	Qualitative	Case Study	Survey	Questionnaire	Interview	Document	Phase
R1		√					√	I
R2	√	√	√	√	√	√	√	I
R3	√	√	√	√	√	√	√	I, II
R4	√	√	√	√	√	√	√	I, II

The research question RQ1 was answered by implementing qualitative methods because it involved analysis of the literature on information security management and strategies. The research question RQ2 was answered by implementing both qualitative and quantitative methods because of the nature of the research question needed to be answered in a bigger picture from many respondents in a short time, access large collection of documents from different organisations. The same is true for the research question RQ3. But, in this case the answer involved finding cultural factors that influenced information security in the case study. The research question RQ4 depended on answers of research questions RQ1, RQ2 and RQ3.

3.4.1 Questionnaires for Phase I

In Phase I there were four questionnaires with structured questions. Three of them were designed with close-ended questions based on ISO27002:2005 code of practice. In this research, we used ISO27002:2005 because it has used simple language and has been adopted in many countries. The questions were measured on a Likert-scale with five-points whereby 1 represented "strongly disagree", 3 represented "undecided" (neither agree nor disagree) and 5 represented "strongly agree". We use Likert-scale in order to measure attitudes and feelings of the respondents about information security. ISO27002:2005 contains 133 technical and non-technical security controls. Questionnaires were distributed to management staff, IT staff and general staff who use computers. The questionnaires are available in Appendix A-C. The fourth questionnaire is designed to gather information on web security and was designed by consulting OWASP and ISO27002:2005 practices. OWASP practices were used because they have been successful in creating secure web applications especially regarding the minimising the security failures for online applications and they under open source license. This questionnaire had closed-ended questions with "Yes", "No" and "Don't Know" scales to get facts about web security in the organisations. The questionnaire was distributed to IT staff responsible for managing their organisation's website. The questionnaire is available in Appendix D.

3.4.2 Questionnaires for Phase II

Phase II was designed in response to the outcome of results from Phase I. There were two questionnaires in this phase for gathering data on national culture dimensions and organisational culture dimensions. The questionnaire for gathering data on national culture dimensions adapted a questionnaire from the GLOBE study on societal culture dimension (Javidan et al, 2004). The GLOBE study has more cultural dimensions than all other studies and it was grounded by integration of implicit leadership theory, value/belief theory of culture, implicit motivation theory, and structural contingency theory of organisational form and effectiveness. The questionnaire was measured using a 7-point Likert scale. The respondents were asked to rank items from 1 (substantially agree) to 7 (substantially disagree). In this research questionnaire is adapted from GLOBE study because they have more dimensions of culture compare to other studies. The second questionnaire was Organisational Culture Assessment Instrument (OCAI) adopted from Cameron and Quinn (1999). Both questionnaires had closed-ended questions. The questionnaire for national culture was analysed using frequencies as suggested by

Jamieson (2004). The questionnaire for organisational culture was analysed using method proposed by Cameron and Quinn (1999). In this research OCAI is used because many organisations used OCAI to measure their culture as mentioned in the literature review. The questionnaires are available in Appendix F-G.

3.4.3 Interviews for Phase I

There was one structured interview. The interview was structured to gather data on threats facing participating organisations. The interview was designed by consulting ISO/IEC 27005:2008 guide. This guide has used simple language, which makes it easy to follow. This interview targeted IT staff or IT managers. The interview was conducted face-to-face with the respondents. The interview contained a mix of closed-ended and open-ended questions. The interview last between two to three hours and was recorded in an interview guide.

3.4.4 Interviews for Phase II

There was a semi-structured interview to gather deep-rooted issues facing information security governance in participating organisations. The participants in this interview were IT staffs that have good knowledge of their organisations' operations. The interview was conducted in face-to-face with the respondents. The interview contained open-ended questions. The interview took three hours and was recorded in a notebook.

3.4.5 Published documents

In this research, secondary data sources were used. Yin (2003) recommends the use of more than one data source. Triangulation is a method whereby more than one data source is used in a research. The secondary data sources that were used in this research were newspapers, public documents, employment contracts, policy documents, legal documents, newspapers and annual reports. The documents were identified by looking into items involving information security in their contents.

3.4.6 Pilot study

A pilot study is defined as a preliminary trial of some or all aspects of the instrument to ensure that there are no unanticipated difficulties (Alreck and Settle, 1995). In this study, the research instruments were pretested in the United Kingdom with four students from Zanzibar who are employees of the Zanzibar public sector. Some deficiencies were raised during the pilot study such as difficulty in understanding the questions in the cultural instrument and the time it took to fill the questionnaires. Also, some typographical issues were raised.

3.4.7 Case study organisations

The case study was conducted on non-profit organisations. The researcher selected public sector organisations that have adopted information systems of a sufficiently high standard to be in a good position to provide relevant data on information security. Permission to conduct research in Zanzibar was granted by the Second Vice President's Office in Zanzibar, which enabled access to the organisations that participated in the research. Each organisation introduced the researcher to their members who agreed to participate in the study. Ten organisations participated in Phase I and nine organisations participated in Phase II. The researcher visited each organisation and personally distributed the questionnaires to participants. During the visit, the researcher conducted interviews and site observations. Participants involved in the Phase I were selected based on their availability to participate in the study. Participants involved with cultural study were randomly selected using a random number generator (Graziano and Raulin; 2007). Table 3.4.2 shows the employees who accepted to participate in the research. These employees were numbered from 1 to N where N was the total number of potential participants and using the random number generator by PS (2012) the participants whose number appeared were given questionnaires as shown in the table 3.4.4. Details of the participants were stored in the research database. Table 3.4.2, Table 3.4.3, Table 3.4.4 and Table 3.4.5 presented the distribution of respondents involved in the study.

The ten organisations involved in the investigations are Marine and Coastal Environmental Management Project (MACEMP), Zanzibar Electoral Commission (ZEC), Zanzibar Revenue Board (ZRB), Ministry of Health (MH), State University of Zanzibar (SUZA), Zanzibar Identity Office (ZIO), Zanzibar Social Security Fund (ZSSF),

Table 3.4.2: Random Selection

Participating Organisations	Phase II - Willing Participants for Randomisation	
	Questionnaire V	Questionnaire VI
POFEDP	8	8
ZSSF	8	8
ZRB	7	7
MEVT	7	11
MH	8	8
ZEC	5	5
ZIO	6	6
RGO	5	7
SUZA	8	9
TOTAL	**62**	**69**

Table 3.4.3: Number of respondents in the participating organisation in Phase I

Participating Organisations	**Phase I – Respondents Returned Questionnaires/Respondents Given Questionnaires**				
	Questionnaire I - Management	Questionnaire II – IT Staff	Questionnaire III – Computer User	Questionnaire IV – Website Manager	Interview – IT Manager
POFEDP	3/3	5/5	6/7		1/1
ZSSF	2/2	2/3	3/3	1/1	1/1
ZRB	1/2	2/3	3/4	1/1	1/1
MEVT	1/2	2/3	4/6	1/1	1/1
MH	1/2	2/3	4/5	1/1	1/1
ZEC	1/2	1/2	3/4	1/1	1/1
ZIO	2/2	2/3	2/3		1/1
MACEMP	1/1	2/3	3/5		1/1
RGO	2/2	2/2	4/6		1/1
SUZA	2/2	3/3	5/7	1/1	1/1
TOTAL	16/20	23/30	37/50	6/6	10/10

Table 3.4.4: Number of respondents in the participating organisations in Phase II

Participating Organisations	**Phase II –Respondents Returned Questionnaires/Respondents Given Questionnaires**		
	Questionnaire V – National Culture	Questionnaire VI – Organisational Culture	Interview – Complex Societal Issues
POFEDP	4/6	5/7	2/2
ZSSF	6/6	6/7	2/2
ZRB	4/5	4/6	2/2
MEVT	4/6	8/10	2/2
MH	5/7	5/7	2/2
ZEC	4/4	3/4	1/1
ZIO	5/5	5/5	2/2
RGO	4/4	4/6	1/1
SUZA	5/7	5/8	3/3
TOTAL	41/50	45/60	17/17

Table 3.4.5: Number of employees in the participating organisations

Participating Organisations	**Number of Employees**
SUZA	250
ZRB	170
ZSSF	75
MACEMP	160
MH	3500
MEVT	13,500
ZEC	77
ZIO	130
POFEDP	752
RGO	64

President Office Finance, Economics and Development Planning (POFEDP), Registrar General Office (RGO) and Ministry of Education and Vocational Training (MEVT). The organisations were chosen base on availability of major information systems in their organisations. After Phase I, MACEMP had its activities terminated after a project that established it ended. The service provided by each organisation is described as follows:

- MACEMP – a public organisation responsible for management of rural coastal population. It provides assistance on agricultural and fisheries issues to people living in the coastal area.
- ZEC – a public organisation responsible for managing elections. It provides services that involve the registration of voters and administration of the voting process.
- ZRB – a public organisation responsible for revenue collection. It provides services involving administration of taxes and tax payers.
- MH – a government ministry responsible for management of health services. It provides administration of hospitals, health workers and patients.
- SUZA – a publicly owned institution of higher education.
- ZIO – a public organisation responsible for administration of registration of Zanzibaris and issuing of Zanzibari identity card.
- ZSSF – a public organisation responsible for administration of pension funds.
- POFEDP – a government ministry responsible for administration of public finance.
- RGO – a public organisation responsible for registration of vital events, businesses, marriage/divorce, properties, and birth/death. It provides administration of inheritance and insolvency. In addition, it keeps registers and index books.
- MEVT – a government ministry responsible for administration of education services. It manages schools, teachers and teacher training colleges.

3.4.8 Analysis of data

According to Yin (2003) analysing qualitative data is about examining, categorising, tabulating and recombining the empirical data to address the initial relationships as identified in the theoretical framework and to further identify new concepts and relationships. Case study generates a vast amount of data that require to be analysed with appropriate tools in order to be meaningful. The data collected in this research was analysed using SPSS software and interviews were manually analysed by the researcher or with the use of Excel software if needed. Documents such as newspapers, public

documents, employment contracts, policy documents, legal documents, and annual reports were manually analysed by the researcher. In this research, both deductive and inductive approaches are used in the analysis of data. Inductive approach is used when a researcher has a loose research question rather than a strict hypothesis. Deductive approach leads investigators to measure relative attainment of predetermined, clear and specific objectives. Inductive reasoning leads investigators to focus more on a program or a product impacts and consequences. In this research, deductive approach was applied when analysing quantitative data because the researcher has not hypothesis but research questions. The inductive approach was used in analysing qualitative data because the researcher focused on the impacts and consequences of culture in the governance of information security. In addition, Jamieson (2004) was consulted concerning the analysis of data. SPSS software was used to provide frequencies of responses for each question for questionnaires in Appendices A-D. The questionnaires in Appendices A-C were tested to find significant differences among organisations in their responses for each question using non-parametric Kruskal-Wallis test provided by the SPSS software. Non-parametric test is used for a sample that has ranked order such as Likert-scale data.

3.4.9 Research validity and reliability

According to Yin (2003) the quality of case study research depends on the satisfaction of numerous criteria that have to be taken into account. These criteria are: construct validity, internal validity, external validity and reliability. Construct validity is "the degree to which the theory or theories behind the research study provide(s) the best explanation for the results observed" (Graziano and Raulin; 2007, p. 181). In this study, multiple source of data collection were used which are questionnaires, interviews, documents and site investigations. The sources were moulded according to already known theories as explained in the previous sections. Also, several organisations were measured in the study.

Internal validity is concerned with cause-effect or causality relationship. Eisenhardt (1989) suggested that linking the emergent theoretical propositions to the existing literature enhances the internal validity of theory building from case study research as applied in this study. Also, this experiment was conducted in the field. "External validity refers to the degree to which researchers are able to generalise the results of a study to other participants, conditions, times, and places" (Graziano and Raulin; 2007, p. 182). In this study, a comparative study among organisations involved in the study during answering of the research question on the state of information security was performed.

Also, a comparative study was performed to compare the findings in this study and findings in the literature.

Reliability is the extent in which measurements remain consistent when the experiment is repeated. Yin (2003) suggests the development of the case study designs and database to ensure reliability in the case study research. In this research, a case study design has been developed and employed. The research can be repeated in non-profit organisations in the developing countries because the experiment was conducted in a bigger picture where all the components derived from the case study were inserted into the picture to provide a solution to the main research problem.

3.5 Reasons behind the choice of methodology

In this project qualitative, quantitative and case study approaches are combined together to perform the research. The quantitative methods enabled to gather data from a large sample quickly. In the next stage information security was investigated through observation of users and their surroundings; and analysed documents. In that stage qualitative methods were deployed. This provides quality data even from a smaller sample. The case study approach enabled the researcher to gather data from a natural setting of the sample.

In Phase I of this thesis, a cross-sectional survey was deployed. The cross-sectional survey enabled to compare the performance of each organisation in the study and at the same time avoided interference with the participants in the research.

In this thesis, a quantitative approach was used for data collection because of the need to gather data from a large sample in a short time. Quasi experiment was used because of respondents were few due to their specific skills required which is user of computers, IT workers or managers. The survey used to gather data was a cross-sectional survey because of the available resource to the researcher, and the need to compare the performance of organisations participated in the study. Questionnaires were used with closed-ended questions to make the data collection process quicker. The questionnaires were distributed personally by the researcher and were self-administered by the respondents. Also, a structured, face to face interview was used to gather data in an efficient way.

In both phases of the project, a qualitative approach was used which suited the small sample size. It was used to study the participants' experiences, meanings and views of the

problem under the investigation. This approach is beneficial where an in-depth understanding of a phenomenon is needed that means to answer the question in a bigger picture. In addition, qualitative methods provide the answer to the "why question" and are suitable for smaller population of respondents. Case studies were utilised as well as a methodology. This is because case studies inspect a phenomenon in its natural setting; utilizing multiple approaches of data collection to collect information from one or a few sources; and there are no clear boundaries between phenomenon and circumstance; they can be used in answering questions of "how" and "why"; or if an investigator cannot manipulate the behaviour of participants in the research (Yin, 2003). The unit of analysis in this thesis is non-profit organisations in a developing country because of scarcity of research in information security for this unit. This thesis will cover an exploratory case study. The lack of research in information security in the context of Zanzibar rationalises a selection of exploratory case study for this thesis hence this is why this type of approach is most relevant.

In this thesis, there was no examination of hypotheses, and any initiation of dependent or independent variables. The intention of the investigator is to understand cultural factors that influence the management of information security. Zanzibar has a population of people immigrated from different parts of the world, with different culture and ethnicity. The researcher was directly involved in the process of data collection and analysis. Also, the researcher was in close contact with the respondents. The researcher did develop the framework of information security culture with the help of the participants. This justifies the selection of the interpretive case study for this thesis.

In this thesis, the data was collected through questionnaires, structured interviews, semi-structured interviews from members of organisations; through site observations and from organisational documents, and public documents. There were two phases of data collection in this study. Phase I involved data collection for answering the research question RQ2. The Phase II of data collection investigated the answer for the research question RQ3. Both phases were used in answering the research question RQ4. Questionnaires gathered quantitative data; interviews, document reviews and site observations gathered qualitative data.

In this project, questionnaires were designed with structured questions and close-ended questions based on ISO27002:2005 code of practice, OWASP guidelines, OCAI guide, and GLOBE study. ISO27002:2005 was used because it has used simple language and has been adopted in many countries. OWASP practices were used because they have been

successful in creating secure web applications especially regarding the minimising the security failures for online applications. OCAI guide was used because it was used by many organisations to measure their culture. GLOBE study questionnaire was used because it has more dimensions of culture than other studies, and grounded by many theories. Some of the questionnaires were measured on a Likert-scale with five-points and seven-points to measure perception of the participants. The other questionnaires were measured using "Yes/No", "Don't Know", "Now/Preferred" scales to get facts from the participants in the organisations.

In this thesis, there were two interviews. There was a structured interview with both open and closed-ended questions. This is because the researcher wanted to get facts and opinions from respondents. The other interview was semi-structured with open-ended questions designed to measure opinions of the participants. The structured interview was based on ISO 27005:2008 guidelines. ISO27005:2008 was used because it has used simple language and has been adopted in many countries for risk assessment. The semi-structure interview was used to capture deep-seated issues facing information security governance in Zanzibar.

In this research, the participants in Phase I of the research were no selected randomly but based on their availability, skills and role. The participants of cultural study in Phase II of the study were selected randomly. This random selection helps to reduce biasness. In addition, the organisations that participated in the study were selected based on availability of information systems of significant high quality in their organisations.

In this thesis, construct validity was ensured by using multiple sources of data gathering. The internal validity was guaranteed by employing a case study, and data collection was done in the field. Also, a comparative study was done among organisations in the case study. The external validity was ensured, by performing a comparative study of findings in this study and studies in the literature. The reliability of the study was guaranteed by the focus to a case study, which is a non-profit organisation in Zanzibar.

3.6 Conclusion

This chapter presented the research approach of this study. Starting from the philosophical approach of the researcher the explorative, interpretive case study approaches have been developed and used for this research project. Data was collected through quantitative and qualitative methods. Also, there was data from a secondary

source. Data gathering procedures ensured validity and reliability of the results. Finally, the reasons for the choice of the methodology have been presented.

The next chapter, Chapter 4, presented the findings from Phase I of the research.

CHAPTER 4

4 ANALYSIS AND RESULTS (PHASE I)

4.1 Introduction

This chapter presents an analysis of the data collected to investigate the state of information security in Zanzibar. Section 4.2 provides a detailed analysis of data collected to form a view of the state of information security in the public sector. The findings presented in Section 4.2 are derived from questionnaires; face to face interviews, documents review, and site observation (see Section 3.4). The research aims at improving information security management by identifying the current state of information security in the studied environment, and developing a framework for improving information security culture. The findings presented here provide the answer for the research question RQ2. Anonymity for study organisations in the publication of findings is very important. Consequently the organisations in the study will be referred to using pseudonyms (O1, O2, O3, O4, O5, O6, O7, O8, O9 and O10) where the information is sensitive.

Phase I involved a comprehensive overview of the general state of information security in the public sector. Ten organisations were involved in the study from the Zanzibar public sector. The organisation selected for this research had better adoption of IT infrastructure than others. In this part, there were four structured questionnaires and one structured face to face interview. Three of the questionnaires were measured on 5-points Likert-scale, where 1 represents strongly disagree to 5 which represent strongly agree. The questionnaires I-IV and interview guide used in this research are found in Appendix A. The respondents were general staff who are computer users, management staff and IT staff. 20 questionnaires were distributed to management staff and 16 were returned and analysed. 30 questionnaires were distributed to IT staff and 23 were returned and used for analysis. Also, 50 questionnaires were distributed to computer users in which 37 were

returned and analysed (see Table 4.1.1). One of the questionnaires was used to gather data on website security and was designed using Yes/No type questions and targeted IT staff whose responsibility involves managing their organisation's website. Six questionnaires were distributed to the respondents responsible for managing six websites that were operational at the time of conducting this study, and all six questionnaires were returned and analysed. The face to face structured interview involved ten IT staff. In addition, a document review and site observations were conducted to investigate information security practices. The document review included acts of the House of Representatives, law documents, policy documents, employee contracts, organisational documents, government's annual reports and newspapers. This multitude of approaches used to collect primary data allowed a triangulation of data which increases the reliability and validity of research. The results are discussed in the section 4.2.

Table 4.1.1: Questionnaire Distribution and Return

Staff Type	**Questionnaires Distributed**	**Questionnaires Returned**	**%**
Management Staff	20	16	80
IT Staff	30	23	77
General Staff (Computer Users)	50	37	74

4.2 Results of state of information security

This section gives a detailed analysis of data collected to form a view of the state of information security in the non-profit organisations in the public sector. The analysis involved clauses on security policy, organisation of information security, asset management, human resources security, physical and environmental security; communications and operations management; access control, information systems acquisition, development and maintenance; information security incident management, business continuity management, and compliance as recommended by ISO/IEC 27002 best practice. Also, other issues including website security, information assurance, security breaches and legal framework will be investigated.

Using SPSS version 17, an analysis of variance was conducted using the non-parametric Kruskal-Wallis test. This test will provide analysis of how the respondents from each organisation respond to each question. Here, the responses with significant different ($p<0.05$) will be reported. The higher the Mean Ranking (MR) means the respondents for that organisation tend toward agreeing with the statement. Also, the lower the MR means the respondents for that organisation tend toward disagreeing with the statement.

4.2.1 Information security policy

This section presents findings of the implementation of the organisations' information security policy including perceptions of it by organisations' members. The implementation of the information security policy and how organisations members perceived it provides essential data for understanding information security management practices in the organisations. Data sources for this section are questionnaires, informal discussions and documents review. Table 4.2.1.1 shows the results on this section. The results show that 56% of management staff agreed on the presence of information security policies in their organisations, but 84% of general staff were undecided or disagreed or strongly disagreed with this statement. There were significant differences on this statement among respondents in different organisations, where ZIO has the highest Mean Ranking while RGO has the lowest Mean Ranking. That was backed up by 69% of management staff who strongly disagreed or disagreed or were undecided that information security policies are communicated to employees, and 92% of general staff strongly disagreed or disagreed or were undecided that they read the policy. There were significant differences on this statement among respondents in different organisations where POFEDP has the highest Mean Ranking while RGO has the lowest Mean Ranking. In addition, 56% of management and 38% general staff acknowledged that the policies are not reviewed periodically.

Table 4.2.1.1: Information security policy (Questionnaires I-III in Appendix A)

Statement	**Type of Respondent (no of respondents)**	**Strongly Disagree %**	**Disagree %**	**Undecided%**	**Agree %**	**Strongly Agree %**	**Organisation responsible for probability $p<0.05$ and their mean rank (MR)**
There is an information security policy for the organisation.	Management staff (16)	6.3	25.0	12.5	31.3	25.0	-
There is an information security policy in place.	General staff (37)	16.2	16.2	51.4	13.5	2.7	p =0.003, MR_{min} = 5.0 (RGO), MR_{max} = 35.5 (ZIO)
I have read the Information security policy.	General staff (37)	35.1	32.4	24.3	8.1		p =0.008, MR_{min} = 7.0 (RGO), MR_{max} = 31.0 (POFEDP)
Information security policy is conveyed to all the employees.	Management staff (16)	12.5	43.8	12.5	25.0	6.3	-
Information security policy is periodically reviewed.	Management staff (16)	31.3	25.0	12.5	31.3		-
Information security policy is periodically reviewed.	General staff (37)	18.9	18.9	54.1	5.4	2.7	-

It was observed that many policies are not documented properly. At present, a main method of delivering the policy to employees is through a letter that is circulated in an organisation. Employees who could not have access to the letter may lack awareness on the existence of the policy. The letter is then filed and stored in a document room out of reach of general staff. In a notable example, the information security policy document for organisation O8 has been marked with the word "Confidential" in its front page. This policy was developed by a contractor who supplied software to the organisation O8.

4.2.2 Organisation of information security

This section presents findings of organisation of information security clauses including perceptions of it by an organisation's members. The organisation of information security provides important data for understanding information security management practices in the organisation. Data sources for this section are questionnaires, informal discussion and documents review.

The results in this section are shown in the Table 4.2.2.1. The results show that the majority of the organisations in the study do not have departments that coordinate information security. Organisation of information security is left to IT technicians to manage. The majority of organisations do not have a specific budget for an information security program and are not capable of implementing an awareness program as 56% of respondents disagreed or were undecided that there is a budget for information security program in their organisations, and 63% disagreed or were undecided to the statement that their organisations are capable of implementing information security awareness program. The researcher learned through informal discussion with some respondents that the budget for information security is integrated into the ICT budget by their organisations. In the study environment, there are organisations that have not defined and documented information security roles for their employees as 50% of respondents disagreed or were undecided on the statement that their organisations defined and documented information security roles. In addition, 50% of respondents feel that organisations in the study have no confidential or non-disclosure agreement and 68% of the respondents feel that they have not signed them. Also, 69% of the respondents in the study feel that their organisations do not conduct security reviews but have procedures in place to contact the authority. The analysis shows that there were no significant differences among the organisations in this clause.

Table 4.2.2.1 - Organisation of Information Security (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %
There is an information security committee in place.	Management staff (16)	25	37.5	12.5	12.5	12.5
There is a budget for information security program.	Management staff (16)	31.3	12.5	12.5	37.5	6.3
The organisation is capable of implements information security awareness program.	Management staff (16)	6.3	37.5	18.8	18.8	18.8
The organisation defined and documented all information security roles.	Management staff (16)	6.3	18.8	25.0	43.8	6.3
There is some confidentiality or non-disclosure agreement for protection of information asset.	Management staff (16)	6.3	31.3	12.5	31.3	18.8
I have signed confidentiality or non-disclosure agreement for protection of organisation's information assets.	General staff (37)	24.3	37.8	5.4	29.7	2.7
There is some procedure in place that specifies how to contact authority (e.g police)	Management staff (16)		18.8	18.8	43.8	18.8
The organisation conducts independent information security review.	Management staff (16)	6.3	43.8	18.8	25.0	6.3

Table 4.2.3.1: Asset Management (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %
There is an inventory of assets.	Management staff (16)		12.5		43.8	43.8
The inventory of assets includes software assets.	Management staff (16)		18.8	18.8	37.5	25
There is information classification in the organisation.	Management staff (16)	6.3	6.3	6.3	56.3	25

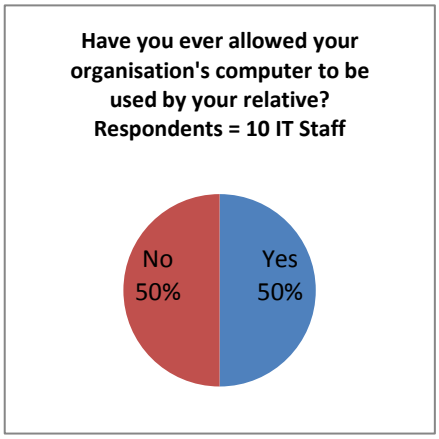

Figure 4.2.3.1: Sharing of Computer (Interview I)

4.2.3 Asset Management

This section presents findings of management of assets including perceptions of it by an organisation's members. The management of assets provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires, site observations and informal discussion.

Assets belonging to the organisations in the study include but are not limited to financial assets such as pension funds, payroll, custom duties and taxes; equipment, furniture, firearms; educational assets such examination records, and educational certificate; and

information assets such as birth and death records, health records and employees records. This clause was in place before the introduction of ICT in the study environment. The result shows that many controls are in place as shown in the Table 4.2.3.1. The Table 4.2.3.1 shows that there is 37% of respondents who have not included software as among the assets, and 19% of the respondents have not classified their organisations' information. Observational data revealed that computers and other equipment have labels for identifying their ownership. The researcher observed that there were a number of

Table 4.2.4.1: Human resources security (Questionnaires I-III)

Statement	**Type of Respondent (no of respondents)**	**Strongly Disagree %**	**Disagree %**	**Undecided%**	**Agree %**	**Strongly Agree %**	**Organisation responsible for probability $p<0.05$ and their mean rank (MR)**
There is a periodically awareness and training program in information security.	Management staff (16)	18.8	37.5	6.3	18.8	18.8	-
There is a periodically awareness and training program in information security.	General staff (37)	13.5	40.5	35.1	8.1	2.7	-
I receive information security awareness training regularly.	General staff (37)	29.7	56.8	2.7	5.4	5.4	-
There are qualified network and system administrators.	IT Staff (23)		30.4	8.7	47.8	13.0	-
There is a disciplinary action against the non-compliant employee.	Management staff (16)	6.3	12.5	18.8	43.8	18.8	-
There is a disciplinary action against the non-compliant employee.	General Staff (37)	5.4	8.1	18.9	45.9	21.6	-
There is a background verification check for candidates of employment and third party.	Management Staff (16)		25.0	18.8	31.3	25	-
My background has been verified.	General Staff (37)	8.1	10.8	40.5	29.7	10.8	-
Terms and conditions of employment include an item about information security.	Management Staff (16)		12.5	31.3	37.5	18.8	-
I agreed and signed terms and conditions of employment that includes responsibilities for information security	General Staff (37)	21.6	27.0	8.1	35.1	8.1	p =0.038, MR_{min} = 10.5 (MACEMP), MR_{max} = 32.0 (ZIO)
I was provided with information security expectation of my position.	General Staff (37)	18.9	35.1	24.3	13.5	8.1	p =0.004, MR_{min} = 6.5 (RGO), MR_{max} = 34.0 (ZIO)
Security roles and responsibilities are defined, documented, and conveyed to would be employees.	Management Staff (16)	6.3	18.8	18.8	50.0	6.3	-

instances where employees who have not been assigned computers used them with the permission of fellow users and using users' accounts. Also, the interview data show that some employees would allow their relatives access to organisations' computers as shown in the Figure 4.2.3.1.

4.2.4 Human resources security

This section presents findings of human resources security including perceptions of it by an organisation's members. The security of human resources provides important data for understanding information security management practices in the organisation. Data sources for this section are questionnaires, face to face interviews, and document review.

The results in this section are shown in the Table 4.2.4.1 and 4.2.4.2. The results show that many respondents feel that their organisations do not provide information security training and awareness regularly. Also, many of the respondents have not received training and awareness in information security on a regular basis. Table 4.2.4.2 shows the qualifications of IT staff in the case study. The case study lacks qualified professional information security personnel.

The results show that many respondents agreed that there is disciplinary action against non-compliance. The statute (Zanzibar, *Public Service Act 2010*) stipulates that a breach of public service and professional code of conduct will trigger disciplinary proceedings. The act defines the public service code of conduct to include the preservation of confidentiality about official dealings, conflict of interest, use of inside information and compliance with the law. The Act was introduced in Zanzibar to comply with

Table 4.2.4.2: IT Staff Qualifications – (Interview I)

Organisation	Diploma/Advance Diploma IT/Computing	BSc IT/Computing	Post-Graduate Diploma	MSc IT/Computing	CISSP/SSCP/CISM/Other security professional certification
POFEDP	0	3	3	3	0
RGO	2	1	0	0	0
MEVT	2	6	1	1	0
MACEMP	2	1	0	0	0
ZEC	2	2	1	0	0
ZRB	0	3	0	2	0
MH	2	1	0	0	0
SUZA	2	4	0	1	0
ZIO	5	1	0	0	0
ZSSF	1	2	2	0	0

requirements of adoption of the multi-party democratic system. The Act does not specifically include terms and condition of employment that reflect information security. Also, the Act does not include how to deal with third party and contractors accessing public organisations. Furthermore, the Act does not stipulate how to administer public sector's equipment that is handed to employees. In addition, the researcher noted that the contracts signed by public sector employees do not specifically include terms and conditions of employment that include information security although they include compliance to Zanzibar laws as one of its terms.

The results show that backgrounds of many employees are not checked as 59% of the respondents disagreed or were undecided that their background were checked although 56% of management respondents agreed that there are background checks for employees. Furthermore, 57% of management respondents agreed that terms and conditions of employments include an item about information security. In addition, 57% of general staff respondents have not signed terms and conditions of employment that include responsibilities for information security. There were significant differences among organisations in the study about employees signing the terms and conditions of employment that include information security. ZIO has the maximum mean ranking of 32 while MACEMP has the minimum mean ranking of 10.5.

The results show that 56% of management respondents agreed that security roles are defined, documented, and communicated to employees. In addition, 78% of general staff respondents disagreed or were undecided that they were provided the information security expectation of their position. In this case, there are significant differences among organisations in the study, where ZIO has maximum mean ranking of 34 while RGO has minimum mean ranking of 6.5.

4.2.5 Physical and environmental security

This section presents findings of physical and environmental security including perceptions of it by an organisation's members. The security of building and its environment provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires, face to face interviews, and site observation.

Table 4.2.5.1 shows the results in this section. The results show that the majority of the controls in this clause have been implemented. 41% of the respondents disagreed on wearing their identity cards all the time in their workplaces. There is a significant

Table 4.2.5.1: Physical and environmental security (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
I wear employee identity card all the time inside the organisation's building	General Staff (37)	13.5	27.0		18.9	40.5	p =0.003, MR_{min} = 8.63 (MH), MR_{max} = 30.0 (ZRB, ZEC, ZIO)
Access to my office is through a door that has a lock.	General Staff (37)	5.4	2.7	5.4	40.5	45.9	-
There is a guideline on removal of equipment, information and software	IT Staff (23)	13.0	26.1	4.3	52.2	4.3	-
There is a guideline on ICT equipment disposal or re-use.	Management staff (16)		12.5	12.5	56.3	18.8	-
There is organisation's guideline on working off-site premises with organisation's equipment.	Management staff (16)		18.8	50.0	25.0	6.3	-
There is an emergency generator.	Management Staff (16)				18.8	81.3	-
There is a security perimeter to protect area that contains information and information processing facilities.	Management Staff (16)	6.3	25.0	12.5	37.5	18.8	-

difference among organisations on this statement with ZRB, ZEC and ZIO has the highest Mean Rankings of 30 while MH has the lowest Mean Ranking of 8.6. Also, 69% respondents were undecided or disagreed on availability of guidelines for working on off-site premises. Table 4.2.5.1 show the results on this clause. In addition, as already mentioned in Section 4.2.3, the researcher noted that some of the respondents had given access to organisations' computers to their relatives.

The researcher observed that some organisations in the study environment have reinforced their security by introducing armed security guards, closed-circuit television and electronic locks. In some of the organisations customers can only talk to employees through glass barriers. The researcher observed that computers were not physically locked in all organisations in the study environment. Although there were emergency generators in all organisations in the study, there is a frequent shortage of fuel in Zanzibar. The researcher observed that some of the organisations in the study do not keep records of visitors or serious in recording the visitors in their organisations. In one of the organisations visitors are screened through a metal detector. In addition, the researcher

observed that security personnel are not checking the validity of visitor's identity in the study environment.

4.2.6 Communications and operations management

This section presents findings of communications and operations management including perceptions of it by an organisation's members. The communications and operations management provide critical data for understanding information security management practices in the organisations. Data sources for this section are questionnaires, site observations and face to face interviews.

The results show that many controls in this section were not implemented (refer to Table 4.2.6.1). These controls are technical in nature. 78% of the respondents disagreed or were undecided that there are guidelines for acceptance of new information systems. Also, 83% of the respondents disagreed or were undecided that there is a separation of development, test, and operational facilities in their organisations. 87% of the respondents disagreed or were undecided that their organisations have policies for protecting electronic messages. Also, 73% of the respondents disagreed or were undecided that their organisations have rules for usage of email and access of internet. There is a significant difference among organisation on this issue where MH has the lowest Mean Ranking of 8.5 and POFEDP has the highest Mean Ranking of 31.8. Furthermore, 83% of the respondents disagreed or were undecided that their organisations have guidelines for network operations and 65% of the respondents disagreed that there are guidelines to keep audit logs recording user activities, exceptions, and information security events. In addition, 61% of the respondents disagreed that their organisations identify and document security features, service levels, and management requirements of all network service. 75% of the respondents agreed that their organisations have backup policy for information and software. However, 57% of the respondents disagreed or were undecided that they had only one role in their employment. There is a significant difference among organisations on this statement where MEVT has the lowest Mean Ranking of 10.9 while ZRB has the highest Mean Ranking of 28.5. 78% of the respondents feel that their organisations lack guidelines on removable media.

Table 4.2.6.1: Communications and operations management (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
There is a guideline for acceptance of new information systems.	IT Staff (23)	8.7	47.8	21.7	8.7	13.0	-
There is a policy to protect electronic messaging.	IT Staff (23)	39.1	43.5	4.3	13.0		-
There is a separation of development, test, and operational facilities.	IT Staff (23)	17.4	52.2	13.0	8.7	8.7	-
There is a policy for prohibiting use of unauthorised software	IT Staff (23)	17.4	60.9		8.7	13.0	-
There is a network operational guideline.	IT Staff (23)	21.7	39.1	21.7	17.4		-
There is a backup policy for information and software	IT Staff (23)		12.5	12.5	56.3	18.8	-
The security features, service levels, and management requirements of all network services have been identified and documented.	IT Staff (23)	26.1	34.8	8.7	26.1	4.3	-
There are rules for using electronic mail and Internet.	General Staff (37)	24.3	27.0	21.6	16.2	10.8	p =0.013, MR_{min} = 8.5 (MH), MR_{max} = 31.8 (POFEDP)
I have only one role in my employment.	General Staff (37)	8.1	40.5	8.1	37.8	5.4	p =0.035, MR_{min} = 10.9 (MEVT), MR_{max} = 28.5 (ZRB)
System administrator and system operator activities are logged.	IT Staff (23)	4.3	21.7	13.0	39.1	21.7	-
There is a guideline to keep audit logs recording user activities, exceptions, and information security events.	IT Staff (23)	26.1	39.1	8.7	4.3	21.7	-
There is a removable media guideline.	IT Staff (23)	34.8	43.5		17.4	4.3	-

4.2.7 Access control

This section presents findings of access control including perceptions of it by organisations' members. The access management provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires and face to face interviews. Table 4.2.7.1 and Figure 4.2.7.1 show the results. The results show that 56% of management staff's respondents agreed the presence of access control policies in their organisation. However, 57% of IT staff's respondents disagreed with the same statement. 70% of the respondents disagreed or were undecided that access rights are reviewed, and 70% of the respondents disagreed or were undecided that routing implementation is used to enforce the access

Table 4.2.7.1 – Access Control (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
There is an access control policy.	Management Staff (16)		18.8	25.0	50.0	6.3	-
There is an access control policy.	IT Staff (23)	26.1	30.4		34.8	8.7	-
There is routing implementation to enforce access control policy.	IT Staff (23)	13.0	39.1	17.4	26.1	4.3	-
There is a review of user access rights periodically.	IT Staff (23)	13.0	34.8	21.7	26.1	4.3	-
There is a system to manage passwords.	IT Staff (23)	17.4	39.1	4.3	30.4	8.7	-
There is a user password guideline.	IT Staff (23)	13.0	52.2	4.3	17.4	13.0	-
There is a clear desk and clear screen policy.	IT Staff (23)	56.5	17.4	17.4	4.3	4.3	-
I have read clear desk and clear screen policy.	General Staff (37)	43.2	24.3	21.6	10.8		p =0.012, MR_{min} = 8.5 (MACEMP), MR_{max} = 35.5 (ZIO)
I use a screen saver that is password protected.	General Staff (37)	13.5	13.5	10.8	37.8	24.3	-
My password contains alphabets and numbers characters.	General Staff (37)	8.1	8.1	10.8	37.8	35.1	-
I am the only person who knows my password for access to organisation's information system.	General Staff (37)	13.5	13.5	13.5	24.3	35.1	-
There is a policy for use of network services.	IT Staff (23)	47.8	17.4	17.4	13.0	4.3	p =0.028, MR_{min} = 6.0 (MACEMP, ZRB, MH), MR_{max} = 22.0 (ZIO)
There is a guideline for system utilities usage	IT Staff (23)	26.1	34.8	26.1	8.7	4.3	-

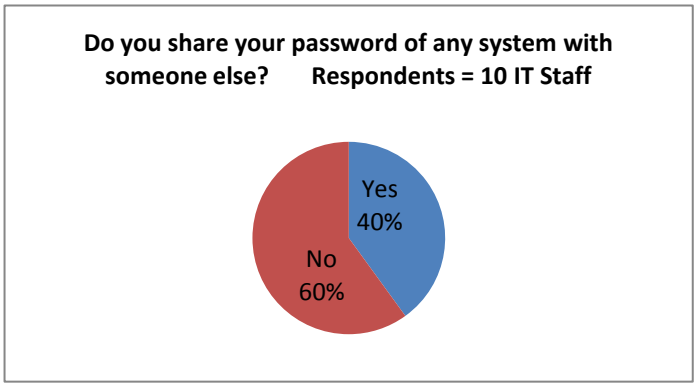

Figure 4.2.7.1: Sharing of Password (Interview I)

control policy. Also, 70% of the respondents disagreed or were undecided that their organisations have guidelines for user passwords and 61% of the respondents disagreed or were undecided that there is a system to manage passwords in their organisations. Moreover, 91% of the respondents disagreed or were undecided that their organisations have policies for clear screen and clear desk. In addition, 89% respondents have not read existing policies and there is a significant difference among organisations on this statement. ZIO has the highest Mean Ranking of 35.5 while MACEMP has the lowest Mean Ranking of 8.5. The results show that 62% of the respondents have awareness on usage of screensaver passwords, and 73% of the respondents create passwords that have combination of alphabets and numbers characters. Also, 40% of the respondents share their passwords with other employees. Moreover, 83% of the respondents disagreed or were undecided that their organisations have policies for use of network services and 87% of the respondents disagreed or were undecided that their organisations have guidelines for usage of system utilities. There are significant differences among organisations on the existence of policies for use of network services as p=0.028. ZIO has the highest Mean Ranking of 22.0 and MACEMP and ZRB have lowest mean ranking of 6.0.

4.2.8 Information systems acquisition, development and maintenance

This section presents findings of information systems acquisition, development and maintenance clause including perceptions of it by an organisation's members. This clause provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires.

The results for this section are shown in the Table 4.2.8.1. The results show that 94% of the respondents disagreed or were undecided that their organisations have policies for the use of cryptographic controls. Also, 57% of the respondents disagreed that they use encryption when sending sensitive information. This is true for both IT and general staff. There are significant differences among organisations on the use of encryption when sending sensitive information by general staff. In this statement ZIO has the highest Mean Ranking of 35 and MACEMP and RGO have the lowest Mean Ranking of 7. In addition, 61% of the respondents disagreed that their organisations have procedures for managing software installation on running systems. 65% of the respondents disagreed that their organisations conduct security risk assessment for message integrity. Also, 61% of respondents disagreed that their organisations carry out technical vulnerability assessments periodically. 58% of the respondents agreed that data output from their organisation's information systems are validated. There is a significant difference

Table 4.2.8.1 – Information systems acquisition, development and maintenance (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
There is a policy on the use of cryptographic control.	Management Staff (16)	31.3	25.0	37.5	6.3		-
I use encryption when sending sensitive information.	General Staff (37)	35.1	18.9	29.7	10.8	5.4	p =0.002, MR_{min} = 7.0 (MACEMP, ZRB), MR_{max} = 35.0 (ZIO)
Encryption is used to protect sensitive information assets.	IT Staff (23)	26.1	30.4		34.8	8.7	-
There are procedures for managing software installation on running systems.	IT Staff (23)	13.0	47.8	4.3	30.4	4.3	p =0.019, MR_{min} = 5.5 (MEVT), MR_{max} = 21.0 (ZIO)
Security risk assessment is applied to ensure message integrity.	IT Staff (23)	30.4	34.8	4.3	17.4	13.0	-
Periodical technical vulnerabilities assessment is carried out and actions are taken to address any found.	IT Staff (23)	21.7	39.1		30.4	8.7	-
Data input to organisation's information systems were validated.	IT Staff (23)	13.0		21.7	47.8	17.4	-
There is a validation of data output from organisation's information systems	IT Staff (23)	13.0	8.7	30.4	34.8	13.0	p =0.028, MR_{min} = 2.83 (SUZA), MR_{max} = 22.0 (ZEC)

among organisations regarding validation of the output data.

4.2.9 Information security incident management

This section presents findings of management of information security incidents including perceptions of it by an organisation's members. The management of information security incidents provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires and face to face interviews.

Table 4.2.9.1 – Iinformation security incidents management (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
There is reporting mechanism for information security incidents	IT Staff (23)	8.7	26.1	8.7	26.1	30.4	p =0.025, MR_{min} = 5.5 (MACEMP, MEVT), MR_{max} = 20.0 (ZIO)
There is a reporting mechanism for information security incidents.	Management Staff (16)		6.3	12.5	56.3	25.0	-
I know where to report information security incidents	General Staff (37)	16.2	5.4	13.5	45.9	18.9	-
There is a guideline for quantifying and monitoring information security incidents.	IT Staff (23)	39.1	34.8		4.3	21.7	-

Table 4.2.10.1 –Business Continuity Management (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %
There is a business continuity plan in the event of a disaster.	Management Staff (16)		31.3	18.8	50.0	
I am aware of organisation's business continuity plans	General Staff (37)	29.7	27.0	29.7	13.5	
Business continuity plans include information security	Management Staff (16)		25.0	37.5	37.5	
Business continuity plans are tested in a regular basis	IT Staff (23)	43.5	30.4	17.4	4.3	4.3

The results are shown in Table 4.2.9.1 and Table 4.2.13.1. 81% of the management respondents feel that their organisations have reporting systems for information security incidents. Although 44% of IT staff respondents disagreed or were undecided about the existence of this system. There is a significant difference among organisations on availability of reporting mechanism from IT staff respondents. Also, 65% of general staff are aware of where to report information security incidents. However, 74% of the

respondents disagreed that their organisations have guidelines on quantifying and monitor information security incidents.

4.2.10 Business continuity management

This section presents findings of management of business continuity including perceptions of it by an organisation's members. The administration of business continuity provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires.

The results are shown in Table 4.2.10.1. 50% of the management respondents agreed that their organisations have business continuity plans in the event of a disaster. However, 86% of general staff respondents disagreed or were undecided that they are aware of the plans. Also, 63% of respondents disagreed or were undecided that the plans include information security and 74% of the respondents disagreed that the plans are tested in a regular basis.

4.2.11 Compliance

This section presents findings of compliance clause including perceptions of it by organisations' members. The clause provides important data for understanding information security management practices in the organisations. Data sources for this section are questionnaires and interviews.

The results are shown in Table 4.2.11.1. 50% of the management respondents agreed that their organisations have guidelines on intellectual property rights. Also, 95% of the respondents among general staff disagreed or were undecided that they are aware of existence of policies on intellectual property rights. In addition, 75% of respondents among management staff feel that their organisations have guidelines on data protection and privacy of personal information. But, 73% of respondents among general staff disagreed or were undecided that their organisations have policies on data protection and privacy. Furthermore, 74% of the respondents disagreed that their organisations have regular checks on technical compliance, and 70% of the respondents disagreed that there is a guideline on information systems audit. There is a significant difference among organisations concerning availability of data protection and privacy policy in their organisations. Also, there is a significant difference among organisations on availability of guideline on information systems audit.

Table 4.2.11.1 – Compliance (Questionnaires I-III)

Statement	Type of Respondent (no of respondents)	Strongly Disagree %	Disagree %	Undecided%	Agree %	Strongly Agree %	Organisation responsible for probability $p<0.05$ and their mean rank (MR)
There is a guideline to ensure intellectual properties rights.	Management Staff (16)	6.3	6.3	37.5	31.3	18.8	-
I am aware of organisation's intellectual property policy.	General Staff (37)	21.6	29.7	43.2		5.4	-
There is a guideline to ensure data protection and privacy of personal information.	Management Staff (16)		12.5	12.5	50.0	25.0	-
There is an organisation's data protection and privacy policy	General Staff (37)	29.7	13.5	29.7	16.2	10.8	p =0.001, MR_{min} = 8.6 (MACEMP,ZRB), MR_{max} = 31.56 (POFEDP)
There is a regular check on technical compliance.	IT Staff (23)	43.5	30.4	8.7	17.4		-
There is a guideline for information systems audit.	IT Staff (23)	26.1	43.5		30.4		p =0.036, MR_{min} = 3.5 (MEVT), MR_{max} = 20.0 (ZEC, ZIO)

Table 4.2.12.1: Website Security (Questionnaires IV)

STATEMENT	YES	NO	DON'T
Does the organisation host the website in-house?	4	2	0
Is there the organisation's guideline for displaying user data in the website?	1	5	0
Does the organisation has guidelines on web application that involves in data collection or transmission?	2	4	0
Does the organisation implement the current Open Web Application Security Project guidelines to protect her website?	0	4	2
Does the organisation in compliance with any web application security standard?	1	3	2
Do you test your web application for security vulnerabilities?	1	3	2
Is there any periodic training in secure coding to organisation's developers?	0	6	0
6 Respondents			

4.2.12 Website security

This section presents findings of website security. Data sources for this section are questionnaires and informal discussion.

The results are shown in the Table 4.2.12.1. The results show that the majority of studied websites are hosted in-house. Most of the organisations in the study do not have guidelines on displaying user data in their website. Also, the organisations lack guidelines on website that involves in data collection or transmission. Furthermore, organisations do not currently implement guidelines from OWASP to protect their website. And many of the organisations are not in compliance with any web application security standard. In addition, websites in the study are not tested for security vulnerabilities. Also,

organisations in the study environment are not providing training in secure coding to their developers in a regular basis. Some respondents commented that their websites depend on security features provided by content management systems they use. According to Kaaya (2004) the websites in the study fall into two categories which are advanced and intermediate level of e-Government.

4.2.13 Security breaches

This section presents findings of security breaches that occurred in the study environment. This section provides essential data for understanding the type of threats facing the organisations in the study. Data sources for this section are interview guide I and informal discussion.

The results are shown in the Table 4.2.13.1. This table shows that a large majority of the organisations in the study have suffered a virus attack. Also, there were few organisations that reported theft of IT equipment. Furthermore, a website belonging to ZEC was defaced during the 2010 elections. The researcher was informed through informal discussions that the virus problem was due to lack of funds for procurement of anti-virus software. Table 4.2.13.2 shows the IT usage in the study environment. The results show that IT usage in the study environment varies depending organisation services.

4.2.14 Information assurance

This section presents findings of information assurance that have been implemented in the study environment. This section provides important data for understanding the type of countermeasure that are offered by the organisations in the study. Data sources for this section are interviews and site observations. Table 4.2.13.1 shows the existing measures implemented in the study environment. The results show that almost all the organisations in the study implemented anti-virus and firewall software. ZIO and ZEC have implemented biometric authentication and encrypted their data. POFEDP has implemented virtual private network (VPN). ZIO and POFEDP have implemented access control card and Personal Identification Numbers (PINs). Also, MH has encrypted its wireless local area network. Unfortunately, there is no organisation that has implemented intrusion detection system or intrusion protection system.

Table 4.2.13.1: Assurance and Breaches (Interview Guide I)

Organisation	Information Systems	Assurance Technology	Breaches
SUZA	Student Information System, Human Resource System, Payroll, Website	Firewall, Anti-virus	Virus, theft
ZRB	Value Added Tax System, Central Motor Vehicles Registration System, Integrated Tax Administration System	Firewall, Anti-virus	
ZSSF	Fund Management Information System, Human Resource System	Firewall, Anti-virus	Virus
MACEMP	Marine Biodiversity Information System	Firewall, anti-virus	Virus
MH	District Health Management Information System, Integrated Human Resource System	Firewall, anti-virus, encrypted WLAN	Virus, theft
MEVT	Education Management information System, Human Resource System	Firewall, anti-virus	Virus
ZEC	Voter Registration System	Firewall, anti-virus, data encryption, biometric aunthentication, Armed Guards	Website defacement
ZIO	Zanzibar ID Registration System	Firewall, anti-virus, data encryption, biometric aunthentication, Armed Guards, Access Control Card, Codelock, CCTV	Virus
POFEDP	Integrated Financial Information System, Payroll System	Firewall, Anti-virus,VPN, Access Control Card, Codelock, CCTV	Virus
RGO	Zanzibar Vital Registration System, Intellectual Properties Automated System	Anti-virus	Virus

Table 4.2.13.2: IT usage (Interview Guide I)

Organisation	Number of Computers	% of Service Computerised	Number of Employees	Services
SUZA	80	20	250	Provide university education
ZRB	120	65	170	Managing tax collection
ZSSF	60	70	75	Managing pension and contributions
MACEMP	40	60	160	Management of rural coastal population
MH	200	60	3500	Treatment and prevention of diseases
MEVT	400	5	13,500	Provide primary, secondary and tertiary education
ZEC	45	20	77	Managing national election
ZIO	40	100	130	Provide identity card to residents of Zanzibar
POFEDP	120	30	752	Managing public finance
RGO	13	10	64	Registration of birth, death, and companies; and administration of inheritance.
Zanzibar GDP	US$561 (POFEDP, 2012)			
Population	1,211,000 (OCGS, 2010)			

4.2.15 Legal framework

This section presents findings of the legal framework that protect the study environment. This section provides important data for understanding the type of legislation that provides protection for the organisations in the study. Data sources for this section are documents.

Zanzibar has several laws that provide protection to information. These laws are: the Laws of Zanzibar, Industrial Property Act 2008, Copyright Act 2003, Zanzibar Broadcasting Act 1997 and Tanzania Communication Regulatory Authority Act 2003.

4.2.15.1 The Zanzibar Penal Decree Act 6 2004

This act criminalises offences against intellectual property, computer equipment or supplies, destruction of computer equipment, interfering with data, interfering with a computer system, illegal interception of data, illegal devices, computer users, and fraud and related activities on government computers.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 373 defines offences of intellectual property which are modifying or damaging or revealing data, programmes or supporting documentation located internally or externally to a computer, computer system, or computer network. This felony is punishable to the maximum of ten years imprisonment.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 374 defines the offence of computer equipment and supplies which involve unauthorised modification of equipment or supplies used or aimed to be used in a computer, computer system, or computer network. This felony is punishable to the maximum of five years imprisonment. If the offence aimed to defraud then the punishment is the maximum of ten years imprisonment.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 375 defines offence of destruction of computer equipment as

> Any person who wilfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever wilfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offence against computer equipment or supplies, and is liable on conviction to imprisonment for a term not exceeding ten years.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 376 defines offences of interfering with data as destroying or modify data, make data worthless or ineffective; disrupt by the lawful usage of data; or denies access to data to any lawful user. This offence is punishable to the maximum of five years imprisonment or a fine or both.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 377 defines offence of interfering with a computer system as obstructs or impedes with the working of a computer system; or obstructs or impedes a user endorsed in using or operating a computer system. This offence is punishable to the maximum of five years imprisonment or a fine or both.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 378 defines offences of illegal interception of data as unlawful interception by technical means of any non-public transmission to or within a computer system; or by electromagnetic emission from a computer system that are carrying computer data.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 379 defines offences of illegal devices as illegal sale, procurement, production or distribution of a device including software made for the aim of committing a felony; a computer password, access code or similar data that can access the whole or any part of a computer system.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 380 defines offences against computer users as:

> Any person who wilfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever wilfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offence against computer users, and is liable on conviction to imprisonment for a term not exceeding five years.

If the offence is committed for the objective to defraud then the punishment is the maximum of ten year imprisonment.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 381 defines offences of fraud and related activity on government computers as unlawful access a computer or exceeding lawful privileges and by that obtained information that is classified for the reason of national defence or foreign relation, or any reason to believe that such

information if obtained could be used to hurt Zanzibar. Unlawful access or excess privileges and thereby acquires financial records of financial institution; information from any government institution; information from any protected computer if the action involves an interstate or foreign communication; unlawful access to non public computer of a government institution; or unlawful access with intent to defraud. These offences are punishable to the maximum of fifteen year imprisonment.

The statute (Zanzibar, *Penal Decree Act 6 of 2004*) in section 179 (1) (f) criminalises internet café owner of misdemeanour if "in any internet centre opened to the public, being the owner allows any person to display any obscene materials from the internet, or being the user displays obscene materials from the internet.*"* This offence is punishable to the maximum of two year imprisonment or a fine.

4.2.15.2 Zanzibar Criminal Procedure Decree

The statute (Zanzibar, *Criminal Procedure (Amendment) Act, 2004*) in sections 111D to 111M have given the magistrate power to authorise police or any authorised person to search computer data or electronic communication for evidence.

4.2.15.3 Zanzibar Industrial Property Act 2008

The statute (Zanzibar, *Industrial Property Act, 2008*) in section 2 covers patents for computer related inventions.

4.2.15.4 Zanzibar Copyright Act 2003

The statute (Zanzibar, *Copyright Act, 2003*) in sections 3 and 15 provides protection for original work involving a computer program.

4.2.15.5 Zanzibar Censorship and Cinematographic Exhibition Act 2009

The statute (Zanzibar, *Censorship and Cinematographic Exhibition Act, 2009*) in section 19 criminalises any person who "make an exhibition by using cinematographic, video cassette, stage play, computer games, entertainment advertisement on poster, motor vehicle with public address system, banners, television or newspaper" without a permit. This offence is punishable to the maximum of six months imprisonment, or a fine, or both.

4.2.15.6 Zanzibar Broadcasting Commission Act 1997

The statute (Zanzibar, *Broadcasting Commission Act, 1997*) regulates and supervises broadcasting activities including radio, television and video broadcastings from Zanzibar or to Zanzibar.

4.2.15.7 Tanzania Communication Regulatory Authority Act 2003

The statute (Tanzania, *Communication Regulatory Authority Act 2003*) is defined as:

> The purpose of regulation of telecommunications, broadcasting, postal services; to provide for allocation and management of radio spectrum, covering electronic technologies and other Information and Communication Technologies (ICT) applications and to provide for its operation in place of former authorities and for related matters.

This act will not cover broadcasting and contents matters in Zanzibar.

4.3 Discussion on research findings

Findings from the case study as presented in the previous section showed that information security governance is an ad hoc practice, lacks planning and lacks management support. There were different security levels of organisation in the study. Also, the findings show that culture has influenced the governance of information security in the case study. The five major levels of concern in the findings are henceforth identified as (i) top management support; (ii) information system structure; (iii) information security controls; (iv) IT usage, information assurance, and security breaches; and (v) legal framework. These five levels will be discussed below in detailed.

4.3.1 Top management support

Findings in Section 4.2.2 showed that information security program lacks a budget, and if there is a budget, then distribution of the available funds face societal challenges. In addition, the information security programmes in the case study lack strategy. Section 4.2.1 revealed that information security policies in the case study are not available; if available they are not reviewed or communicated. These findings are consistent with the one identified by Abu-Musa (2010).

In the literature, it is recommended that management support is crucial for the success of information security program (Ruighaver et al., 2007; Knapp Kenneth and Ford, 2006; Chia et al., 2002). Management must set rules and develop policies for information security.

4.3.2 Information system's structure

The findings in Section 4.2 showed that levels of information systems' structure on organisations in the case study varied. Organisations involved with elections, registration of citizens, and finances have strong security compare to others. This shows that

information security in the case study depends on the criticality of information system in the organisation.

These findings are consistent with the one about information security in financial institutions in the literature (Kankanhalli et al, 2003; NISS, 2007).

4.3.3 Information security controls

The findings in Section 4.2.1 showed that some organisations lacked information security policies; existing policies are not communicated or reviewed. Information security programmes lacked budget. Findings in Section 4.2.2 showed that the organisations lacked the capability to conduct information security awareness training. In addition, Section 4.2.4 showed that many employees lacked information security awareness training and existing training programs are not provided periodically. Also, organisations lacked qualified information security professionals. The findings in Section 4.2.4 showed that policies and disciplinary actions are weakly enforced. These finding are consistent with findings in the literature (Abu-Musa, 2010; Cheang and Sang, 2009; Karokola and Yngström, 2009; Khalfan and Ashawaf, 2003; Kimwele, Mwangi and Kimani, 2010; Mundy and Musa, 2010; Ndou, 2004).

In addition, Section 4.2.8 showed that technical vulnerability assessment is not carried out regularly. Findings in Section 4.2.9 suggested that there are employees who have no awareness of reporting system for information security incidents. In addition organisations lack guidelines on quantifying and monitoring information security incidents. The findings in Section 4.2.10 suggested that business continuity plans are not conveyed to employees, or do not included information security or are not tested regularly. These findings are consistent with findings in the literature (Abu-Musa, 2010).

The findings in section 4.2.11 showed that employees are unaware of existing policies and guidelines such as the policy on data protection and privacy, policy on information security, guidelines on acceptance of new information systems, policy on protection of electronic messages, guidelines on network operations, guidelines on keeping audit logs for user's activities, policy on back-up of software, guidelines for intellectual property rights, guidelines on system audits, and policy on the use of network service. Also, there are employees who are unaware of business continuity plans in their organisations. Information security awareness is very important for employees for an organisation to achieve an effective information security strategy.

The findings in Section 4.2.6 suggested that organisations lack guidelines, policies and rules on various controls such as email, access of internet, network operations; audits logs of users; exceptions and removable media. In Section 4.2.7, respondents felt that access rights policies are not reviewed, and there is lack of guidelines for user passwords. There are respondents who shared their passwords with other employees. The findings in Section 4.2.8 suggested that there is lack of policies for cryptographic controls, and many users do not use encryption. Also, findings in Section 4.2.11 showed that organisations did not provide regular checks on technical compliance and lacked guidelines on information system audits. Findings in Section 4.2.12 suggested that websites use ad hoc practices on security. A lack of policies and benchmarking on information security controls lead employees to use cultural influenced practices that could jeopardise the security of an organisation.

4.3.4 IT usage, assurance, and security Breaches

The findings in Section 4.2.14 suggested that there is low usage of IT in the case study. Also, Section 4.2.13 showed that the measures to protect the organisations that were implemented include anti-virus software, firewall, biometric, encryption, access control cards and Personal Identification Numbers (PINs); and VPN. No organisation in the case study has implemented intrusion detection or prevention systems. Findings suggested that breaches of security were not severe which include theft, virus and website defacing. More measures and breaches of security have been reported in this literature (CLUSIF, 2008; and CSI, 2011; PWC, 2008). Also, the lack of security policies and severity of breaches was consistent with findings by Doherty and Fulford (2005).

4.3.5 Legal framework

Findings in Section 4.2.15 suggested that the case study has various legislations to protect information security. The present legislation include offences against intellectual property, computer users, computer equipment or supplies, destruction of computer equipment, interfering with data, interfering with the computer system, illegal interception of data, illegal devices, computer users, and fraud and related activities on government computers. In addition, there are legislations on: offence against misdemeanour by Internet café owners involving display of obscene material in their premises; power to authorised search computer data or electronic communication for evidence; patents for computer related inventions; copyright protection for original work involving a computer program; regulating and supervising broadcast activities; censorship of exhibition; regulation on telecommunication and postal services. Findings suggested lack of employees' contract

that reflects information security. Also, the present legislation on public service did not specifically include the terms that reflect information security. More legislation for protecting information has been reported in the literature (Bharvada, 2002; Blythe, 2005; Chaturvedi et al, 2008; Moustakas et al, 2005).

4.4 Conclusion of Findings

Overall, an analysis of the study environment revealed that the level of information security can be described by two ways: before computerisation and after computerisation. Also, the analysis revealed that information security can be explained through social and technical perspectives. Table 4.4.1 summarises the findings.

The information security governance seemed to be ad hoc, lack planning and lack management support. Various information security controls lacked policies and guidelines. Many policies are not communicated to employees or reviewed. Although the organisations have qualified IT personnel, they lack professional information security personnel. Physical security employees seemed to be computer illiterate. Organisations are strongly secured physically, although IT equipment is not physically locked and visitors' records are not properly kept. Security levels among the organisations appeared to be different. Technical controls such as access controls, cryptographic controls, network controls among others seemed to be weakly managed. Web applications use ad hoc security. The existing assurance methods include anti-virus, firewall, biometric authentication and electronic locks. However, there is a lack of implementation of intrusion detection and prevention systems. It seems that security breaches are not recorded. And, those recorded have not caused major loss of assets.

Although the legal framework has some legislation that provides information assurance, it lacks legislation on electronic transactions and cybercrimes. It seemed that contracts lack items that specifically identify information security.

As a consequence, the findings appear to suggest that the level of security from the old manual systems is stronger than the new IT systems. At the technical level, information security is weak. Also, the organisations in the study have varied information security level. Many policies and guidelines for various information security controls are nonexistent. The information security governance seemed to be improvised. To understand information security better, the societal context needs to be considered. For example, issues of lack of policies or policies not conveyed to employees need to be investigated. Phase II of data collection was conducted in order to understand the impact

of culture in the governance of information security. Next chapter, chapter 5 presents the analysis and findings on data collected in Phase II of the research.

Table 4.4.1: Overview of study findings

Data Construct	**Findings**
Information security policy	Not available, if available not communicated or not reviewed
Organisation of Information Security	Lack strategy, information security governance is ad hoc and poorly planned
Asset Management	Well organised, not adapted to new technology
Human Resource Security	Lack strategy for training and awareness in information security
Physical and environmental security	Good organisation inherited from manual system; not adapted to new technological environment; poor recording of visitors
Communication and Operations Management	Poorly managed, ad hoc practices, lack guidelines and policies for technical controls; lack strategy, lack benchmarking
Access Control	Poorly managed, lack strategy, lack policies and guidelines for technical controls; lack benchmarking
Information systems acquisition, development and maintenance	Poorly managed, lack policies and guidelines for technical controls; technical vulnerabilities assessment are not carried out; lack strategy, lack benchmarking
Information Security Incidents Management	Ad hoc practices; lack guidelines for monitoring and quantifying information security incidents; lack inclusion of forensic analysis; lack strategy
Business continuity management	Poorly managed, ad hoc practices, lack plans, lack testing; lack strategy
Compliance	Lack of awareness on policies and guidelines; lack checks on technical compliance; lack guidelines on information system audit; lack strategy
Website Security	Poorly managed, ad hoc practices, no bench marking; lack strategy
Security Breaches	Not severe with little financial impact
Legal Framework	Lack in-depth legislation to combat crimes of the digital age
Information Assurance	Not advance, poorly planned; depends on organisation's services; lack strategy
Organisations	Security level is high for organisations that provide services for finance, managing voting and identity registration; policy on adapting to working with new technology has not been implemented
Employees	There is a gap between management and employees in conveying decisions and policies. Management structure lacks integration of information security strategy.

CHAPTER 5

5 ANALYSIS AND RESULTS (PHASE II)

5.1 Introduction

This chapter presents an analysis of the data collected to investigate the societal and organisational issues that impact the governance of information security in Zanzibar. The chapter is divided into six sections. Section 5.2 presents an analysis of data collected to form a view of complex societal issues that affect information security governance in Zanzibar. Sections 5.3 and 5.4 give a detailed analysis of data gathered in order to form a view of the national and organisational culture of public organisations respectively. Section 5.5 presents a cross analysis of information security values and issues identified in the study environment. The final section, section 5.6, provides the conclusion of the chapter. The findings presented here were used to answer the research question RQ3.

The findings presented in this chapter are derived from questionnaires, face to face semi-structured interviews and documents review. Here, the document reviewed included reports, websites and newspapers. The research aims at improving information security management by identifying the organisational and national cultural values and factors that have influenced the implementation of information security management and developing a process model for information security governance based on semiotics. Anonymity for study organisations and participants in the publication of findings is very important for the type of data gathered in this phase. Consequently the organisations and respondents in the study will be referred using pseudonyms if the information is deemed sensitive. Phase II of the research involved two questionnaires, a semi-structured face to face interview and document review. Respondents were from nine public organisations. One of the organisations in Phase I was dissolved by the time we conducted Phase II data collection. The results of the survey are discussed in sections 5.2, 5.3 and 5.4.

5.2 Complex societal issues facing information security

This section presents findings of complex issues that impact the management of information security in the study environment. The section provides important data for understanding the management of information security. Data sources for this section were semi-structured interviews and documents reviews. The interview is found in Appendix A as interview guide II. The interview aim was to discover complex societal issues that affect information security governance in the public sector. 17 senior IT staffs participated in this interview. The main themes here were trust, IT usage, availability of resource, confidentiality of information, enforcement of policies and disciplinary actions, communication among employees and political situation in Zanzibar. The themes are important in understanding the impact of complex societal issues to information security. The results are discussed in the next subsections.

5.2.1 Trust

Trust among employees is important in the organisation. The results show that trust varies among organisations. Respondent [DR3] said:

> "There is no trust involving logging out of computer systems, everybody tries his best to logout. We do loan each other money without contracts."

Respondent [DR14] said:

> "We trust each other here because there are not many employees, this make us know each other. I can leave my computer without logging out. I can loan money to my fellow employee without signing a contract. Some bias is normal when dealing with trust based on nepotism or even people who hailed from the same region."

Respondent [DR13] added:

> "We trust each other here; even we leave our phones in the office. Also, I can leave my computer without logging out in my office."

[DR1] added:

> "I trust my fellow employees; theft among employees is not possible. I trust my fellow employees in such a way I could loan them money without signing a contract. I will leave my computer without logging out; I will let the screensaver

do the work for me. When dealing with repairing computers belonging to big bosses I do not trust other employees to do the job, I will do it myself."

Respondent [DR8] added:

"We trust each other here, I can loan my fellow employee money without contract. I can leave my computer in the office without logging out, but I logout as a policy."

The results show that trust among employees has an impact on information security. In the study environment, trust lead to people not using security features available for them to protect information.

5.2.2 IT usage

The results show that IT usage varied according to organisations in the study. Many employees share few computers available in the study environment. Respondent [DR1] said:

"We do not have enough computers for everyone, but [employees with position XXX] have their own laptops which they do not share, but other employees do share the computers."

Respondent [DR4] said:

"There is low usage of computers and internet especially the internet. Employees share few computers. Our internet bandwidth is very low and sometimes not available."

Respondents [DR10] said:

"Basically usage of computers depends on the individual departments. Not all employee have their own computers, those who do not have direct job description regarding usage of computer are sharing with others. Connectivity is not stable, and employees are not satisfied. Sometimes internet connection is not available. We have two ISP, but there are a lot of complaints about their services. Our bandwidth is a shared 512kbps."

And respondent [DR11] added:

"Usage of computer is low due to lack of IT awareness, and fear of computers. We have high availability of computers but are not used effectively. Internet connection is poor, too many complaints about the internet service."

Respondent [DR17] said:

> "Our internet service has been disconnected due to lack of payment, poor service from ISP and breach of contract on ISP part. We bought dedicated bandwidth, and we were provided with shared bandwidth. Only 70% of employees have their own computers provided by the organisation. Management employees have laptops and other employees have desktops. Management employees get an annual subscription of anti-virus software but other employees may get if there are adequate funds."

The results show that IT usage faces challenges such as few computers, low bandwidth, lack of training, and uneven distribution of resources available among others.

5.2.3 Availability of funds

Availability of funds varies according to organisations in the study. Respondent [DR2] said:

> "Funds availability is very poor; sometimes we only get funds for 10% of the budget. Sometimes we get funds when the activity involves a bigwig."

Respondent [DR15] said:

> "There are problems in getting funds for implementing our daily tasks. If we want to aim high, funds are not available."

Respondent [DR14] added:

> "Availability of funds is very a big issue. We have a budget, but funds are delay or not available at all. There is bureaucracy and corruption in dealing with funds."

Respondent [DR11] said:

> "Funds availability is very slow. There is no budget for IT. Delay is sometimes caused by the person who signs the check; he/she may bias to some people by favouring his/her friends."

And respondent [DR3] said:

> "Availability of funds in the department is a big problem. You may ask for funds to implement an important activity and may not get them. Sometimes there is unequal treatment of employees when it comes to distribution of funds. There is bribery and favouritism based on family, region of birth, even political affiliation."

The results show that availability of fund in the study environment is bounded. Distribution of funds faces issues such as corruption and favouritism.

5.2.4 Collaboration between security and IT personnel

It is very important to have good working relationship between physical security personnel and IT personnel. The results show that physical security personnel have low education and low IT literacy. Also, they are not involved in any other area of information security. Respondent [DR8] said:

> "We have little cooperation with security personnel. Security personnel deal with physical security only. Security personnel do not know anything about login details of any system. We do not consult them during the procurement process of IT equipment or involve them in any other way. Majority of our security personnel are IT illiterate, with low education."

And respondent [DR13] added:

> "We have good cooperation with security staff as our fellow employees. We do not cooperate with them in terms of IT. Security personnel guard our offices only. Their awareness of IT is very little or none at all. However, at [section XXX] the security personnel have some IT awareness because they did attend seminars and training."

The results show that physical security personnel lack IT skills and are not involved in the IT issues.

5.2.5 Confidentiality of information

Confidentiality of information is very important in an organisation. The results show that confidentiality of information varies among organisations in the study. Respondent [DR2] said:

> "There are gossips of information that was not released officially. For example, there was an incident when a student came to me with full information involving the list of sponsored students by the ministry, this information was not released to public, only people who are in the meeting knew about it. So there is leakage of information in this organisation. There are groups of people that gossip for confidential information, for example people who come from Makunduchi, Pemba, and Donge they will gossip among themselves about leaked information. Members of political parties also will gossip among themselves on leaked information especial members of opposition parties."

Respondent [DR7] added:

"Confidentiality of information is low here. For example, management decisions are leaked before the official release. Some members of management staff do leak confidential information to their friends and families. This is because of the delay of the official release of information concerning important decision."

Respondent [DR10] said:

"There is some leakage of confidential information. However, anyone leaked information will be disciplined. Three times we have disciplined employees since I was here."

And *r*espondents [DR11] said:

"Confidentiality is not high, some people may mention about the content of your letter without you giving to them."

The results show that confidentiality is broken by employees to friends and family.

5.2.6 Enforcement of policies and disciplinary actions

Enforcement of policy and disciplinary action is very important in an organisation. The researcher observed that there is a challenge in implementing the existing policies. The results show that policy enforcement and disciplinary action vary among organisations in the study. As respondent [DR1] said:

"There is a lot of hesitation in implementing policies. Employees are afraid of each other when implementing policies. They Fear of being label a bad or unkind boss. We have guidelines here that we try to implement, but employees are not complying with them, so we do not see the need to update them. Enforcement of disciplinary action is low. For example, we do not have employees' attendance records."

Respondent [DR12] added:

"Enforcement of policies is very weak here especially those involving finance are difficult to be implemented. There is bias in implementing policies among groups of people who works here especially those who hailed from the same district."

And respondent [DR3] said:

"I think we lack important policies. There is weak enforcement of policies; people know that they can do anything without being punished. For example, in the past anyone who enters our building will be asked for an identity card, but not anymore. Anybody from outside the [organisation XXX] can come and use the facilities without being questioned. Only administrative employees such as

cleaners are made to comply with policies. There is no bias in implementing policies in the last six months but before there was bias based on political interest although they were done in underground without noticing."

The results show that policies and disciplinary actions are not enforced and face issues of bias.

5.2.7 Communication during problems

Communication among employees when there is a problem is very important in an organisation. Communication is good among employees in the study environment, but there are few cultural issues. As respondent [DR12] said:

> "When dealing with IT problems there are no good communications. However, when dealing with theft, we have good cooperation. There is no good communication between certain groups of people such as those with different political ideology."

And respondent [DR12] said:

> "Communication between employees depends on which part of organisation and section, there is some hesitation in solving a problem so no good communication, if the problem involves a bigwig then the communication will be good in order to solve the problem quicker."

The results show that communication faces prejudice.

5.2.8 Political situation in Zanzibar

It is very important to look at the situation during civil unrest. Since the start of multi-party democracy in 1992 Zanzibar has been marred with violence during elections. Zanzibar has two main political parties which are Chama Cha Mapinduzi (CCM) and Civic United Front (CUF). The results in the Table 5.2.8.1 and 5.2.8.2 show that Zanzibar is divided into two political camps. There is mistrust on the way votes are counted. As the CUF Presidential Candidate Maalim Seif Sharif said:

> "There are two people hidden at Kisiwandui trying to forge election results electronically. We are very careful this time. We would be very careful this time. We wouldn't allow such a thing to happen again. They did in 1995 and cause a lot of problems; they won't be able to do it again this time" (Sadallah, 2010).

Members of CUF believe that they are oppressed by the Revolutionary Government of Zanzibar (Brent and Mshigeni; 2004). This leads to a formation of an Islamic religious

Table 5.2.8.1: 2010 Zanzibar General Election Source: (HOR, 2011)

Party	Number of seats	Island of Constituent
Chama Cha Mapinduzi (CCM)	28	Zanzibar
Civil United Front (CUF)	18	Pemba
Civic United Front (CUF)	3	Zanzibar

Table 5.2.8.2: 2010 Zanzibar Presidential Election (Source: (CS, 2010))

Party	Number of Votes
Chama Cha Mapinduzi (CCM)	179,809
Civil United Front (CUF)	176,338
Others	8,777

awakening organisation call UAMSHO which has been manoeuvred in order to accomplish political objectives (NL-Aid, 2012). CCM has accused UAMSHO of campaigns of violence including "massive destruction of properties and death of an innocent policeman" (Sadallah, 2012). The investigation revealed that the political situation in Zanzibar is not stable, and violence does happen. This could impact information security.

5.3 National culture survey results

The survey was conducted using a structured questionnaire measured by 7-points Likert-scale. Likert-scale was design with 1 representing substantially agree to 7 which represent substantially disagree. The questionnaire was adapted from House et al. (2004, p.30). The questionnaire is found in Appendix F as Questionnaire V. 50 respondents were randomly selected from employees of nine public organisations in Zanzibar. Participants were selected from each organisation based on random selection from a pool of employees willing to participate in the research as shown in the Table 3.4.3. Using the random number generator by PS (2012) the participants were given questionnaires as shown in the Table 3.4.4. 41 questionnaires were returned, and all were suitable for analysis. The results are discussed in the next subsections.

5.3.1 Power distance

The results are shown in the Table 5.3.1. The results show that 61% of respondents agreed that power is shared unequally in practice ("As is"). However, 61% of the respondents disagreed or were undecided that power should be shared unequally ("Should be"). The results show that the majority of respondents feel that power is shared unequal, but they will prefer to be shared equally.

Table 5.3.1: Results of national culture survey (Questionnaire V – Adapted from House et al (2004))

Dimension	Statement	Substantially Agree (%)	Moderate Agree (%)	Slightly Agree (%)	Undecided (%)	Slightly Disagree (%)	Moderate Disagree (%)	Substantially Disagree (%)	Average Score (Likert Value)
Power Distance	Followers are expected to obey their leaders without question. (As is)			61	22	17			3.56
	Followers should be expected to obey their leaders without question. (Should be)	10	20	10	7	10	33	10	4.26
Uncertainty Avoidance	Most people lead highly structured lives with few unexpected events. (As is)	2	20	20	32	10	16		3.76
	Most people should lead highly structured lives with few unexpected events. (Should be)	7	12	22	34	10	5	10	3.83
Humane Orientation	People are generally very tolerant of mistakes. (As is)	7	10	17	15	19	12	20	4.45
	People should be generally very tolerant of mistakes. (Should be)	17	12	20	21	15	10	5	3.55
Institutional Collectivism	Leaders encourage group loyalty even if individual goals suffer. (As is)	17	7	26	20	10	10	10	3.69
	Leaders should encourage group loyalty even if individual goals suffer. (Should be)	27	12	17	12	15	17		3.27
In-group Collectivism	Employees feel great loyalty toward this organisation. (As is)	17	28	15	10	15	10	5	3.28
	Employees should feel great loyalty toward this organisation. (Should be)	20	15	20	15	20	10		3.30
Assertiveness	People are generally dominant in their relationship with each other. (As is)	2	5	35	14	20	12	12	4.29
	People should be generally dominant in their relationships with each other. (Should be)	2	12	22	17	15	12	20	4.47
Gender Egalitarianism	Boys are encouraged more than girls to attain a higher education. (As is)	15	24	17	7	12	20	5	3.57
	Boys should be encouraged more than girls to attain a higher education. (Should be)	7	12	7	10	10	12	42	5.08
Future Orientation	More people live for the present rather than for the future. (As is)	20	28	24	17	2	2	7	2.87
	More people should live for the present than for the future. (Should be)	5	8	29	12	5	7	34	4.61
Performance Orientation	Students are encouraged to strive for continuously improved performance. (As is)	17	37	17	15	2	7	5	2.89
	Students should be encouraged to strive for continuously improved performance. (Should be)	44	24	22	2	5		2	2.05

5.3.2 Uncertainty avoidance

The results are shown in Table 5.3.1. 42% of the respondents agreed that members of society seek orderliness, consistency, structure, formalised procedures, and laws to cover situations in their daily lives. There were 58% respondents who were undecided or disagreed with the previous statement. Also, 41% of respondents agreed that members of society should seek orderliness, consistency, structure, formalised procedures, and laws to cover situations in their daily lives. There are 59% respondents who were undecided or disagreed with the previous statement. The results show that a majority disagreed or were undecided that there is orderliness, consistency, structure, and laws to cover their daily lives in practice and would prefer that way in value.

5.3.3 Humane orientation

The results are shown in Table 5.3.1. 51% of the respondents disagreed that society values and rewards altruism, caring, fairness, friendliness, generosity, and kindness in practice. However, 49% of the respondents agreed that society should value and reward altruism, caring, fairness, friendliness, generosity, and kindness. The results show that the society is not humane oriented but would prefer to be humane.

5.3.4 Institutional collectivism

The results are shown in Table 5.3.1. 50% of respondents agreed that society practices favour to reward collective distribution of resources and collective actions. There were 50% of respondents who either undecided or disagreed with the previous statement. Also, 56% of respondents agreed that society should favour to reward collective distribution of resources and collective actions.

5.3.5 In-group collectivism

The results are shown in Table 5.3.1. 60% of respondents agreed that in practice, this society takes pride in their families or organisations. Also, 55% of the respondents agreed that the values of the society are to take pride in their families or organisations.

5.3.6 Assertiveness

The results are shown in Table 5.3.1 and Table 5.3.2. The results show that 44% of the respondents disagreed that people are assertive and confrontational in practice. However, there are 56% of the respondents who either agreed or were undecided about the previous statement. Also, there are 47% of the respondents disagreed that people should be assertive and confrontational. There are 53% of the respondents who were either agreed or undecided with the previous statement.

5.3.7 Gender egalitarianism

The results are shown in Table 5.3.1. The results show that 56% of the respondents agreed that in practice, there is gender inequality in study environment. However, in values 64% of the respondents disagreed that society should have gender inequality.

5.3.8 Future orientation

The results are shown in Table 5.3.1 and Table 5.3.2. The results show that 72% of the respondents agreed that in the study environment, people are not planning for the future. However, 46% of respondents prefer to plan for the future.

5.3.9 Performance orientation

The results are shown in Table 5.3.1. The results show that 71% of the respondents agreed that in the study environment society rewards members for performance progression and brilliance. Also, in the study environment, society 90% of the respondents agreed that values of the society are to reward members for performance progression and brilliance.

5.3.10 Comparison between Zanzibar national culture and other countries

Table 5.3.2 show the comparison of findings on national culture from this research and the GLOBE Project. Zanzibar results are compared with results from Kuwait, USA and Sweden. Kuwait has a majority of its population as Muslims. USA is a developed country with Capitalist doctrine. Sweden is a developed country and welfare state with market

Table 5.3.2: Comparison of national culture (Source: House et al (2004))

Dimension of Culture	Zanzibar	Kuwait	Sweden	United States of America
Power Distance (Practice)	3.56	5.12	4.85	4.88
Power Distance (Values)	4.26	3.17	2.70	2.85
Uncertainty Avoidance(Practice)	3.76	4.21	5.32	4.15
Uncertainty Avoidance (Values)	3.83	4.77	3.60	4.00
Humane Orientation (Practice)	4.45	4.52	4.10	4.17
Humane Orientation (Values)	3.55	5.06	5.65	5.53
Institutional Collectivism (Practice)	3.69	4.49	5.22	4.20
Institutional Collectivism (Values)	3.27	5.15	3.94	4.17
In-Group Collectivism (Practice)	3.28	5.80	3.66	4.25
In-Group Collectivism (Values)	3.30	5.43	6.04	5.77
Assertiveness (Practice)	4.29	3.63	3.38	4.55
Assertiveness (Values)	4.47	3.76	3.61	4.32
Gender Egalitarianism (Practice)	3.57	2.58	3.84	3.34
Gender Egalitarianism (Values)	5.08	3.45	5.15	5.06
Future Orientation (Practice)	2.87	3.26	4.39	4.15
Future Orientation (Values)	4.61	5.74	4.89	5.31
Performance Orientation (Practice)	2.89	3.95	3.72	4.49
Performance Orientation (Values)	2.05	6.03	5.80	6.14

economy. The results show that Zanzibar has a lower average value for the Power Distance compare to Kuwait, Sweden and USA in terms of societal practices. The average value for Power Distance in terms of societal values is higher for Zanzibar compare to Kuwait, Sweden and USA. Zanzibar has lower average value for Uncertainty Avoidance compares with Kuwait, Sweden and USA in terms of societal practices. Zanzibar has a higher average value for Humane Orientation in comparison to USA and Sweden at societal practices, but, has a lower average value in terms of societal values. Zanzibar has lower average value for Institution Collectivism, In-Group Collectivism, Performance Orientation, and Future Orientation at both societal practices and values in comparison to USA, Kuwait and Sweden. Gender Egalitarianism is higher for Zanzibar at both societal practices and value in comparison to Kuwait and USA.

5.3.11 Conclusion

The results show that the study environment majority feels that power is not shared equally. The majority feels that there are orderliness and laws to protect them. In the study environment, a majority feels that the society is not caring or kind. The results show that society values collective distribution of resources and values family or organisations. A majority feels that society in the study is not confrontational. A majority feels that there is gender inequality in the study environment. In the study environment, a majority feels that society is not planning for the future. Finally, progression and brilliance is rewarded in the study environment.

5.4 Organisational culture survey results

The survey was conducted using an OCAI questionnaire adopted from Cameron and Quinn (1999, p.20-25). 60 questionnaires were distributed to randomly selected respondents from nine public organisations in Zanzibar. Participants were selected from each organisation based on random selection from a pool of employees willing to participate in the research as shown in the Table 3.4.3. Using the random number generator by PS (2012) the participants were given questionnaires as shown in the table 3.4.4. 45 questionnaires were returned, and all were suitable for analysis. The questionnaire is found at Appendix G. The results of the survey on each dimension of organisation culture are shown in the Figure 5.4.1 to Figure 5.4.7, Table 5.4.1 and Table 5.4.2. The figures show mean score of each culture. The analysis of data is adopted from Cameron and Quinn (1999).

5.4.1 Dominant characteristics

Table 5.4.1 and Figure 5.4.1 show that hierarchy culture dominates the firms' characteristics in the study. This shows that the study environment is formalised and structured where procedures govern what people do. There are gaps on the clan and market cultures between current and preferred culture. These points need some attentions to reduce the gap.

5.4.2 Organisational leadership

Table 5.4.1 and Figure 5.4.2 show the mean score on organisational leadership dimension. This dimension is dominated by hierarchy culture where employees considered their leaders to be coordinators and organisers. The employees preferred higher scores on this dimension.

5.4.3 Management of employees

Table 5.4.1 and Figure 5.4.3 show the mean score on management of employees' dimension. This dimension is dominated by the clan culture where teamwork, consensus and participation are the norms. In this culture "people share a lot of themselves" (Cameron and Quinn; 2006, p.66). The respondents preferred higher score on this dimension.

5.4.4 Organisational glue

Table 5.4.1 and Figure 5.4.4 shows the mean score on organisational glue dimension. This dimension is dominated by hierarchy culture. The glue that holds organisations is formal rules and policies. The respondents would prefer a higher value on this dimension.

5.4.5 Strategic emphases

In the Figure 5.4.5.1 shows the scores on strategic emphases dimension. This dimension is dominated by hierarchy culture where emphases are on permanence and stability. Respondents would prefer higher value on this dimension.

5.4.6 Criteria for success

Finally, the dimension for criteria of success is shown in Table 5.4.1 and Figure 5.4.6.1 Clan culture dominates this dimension where success is determined based on development of human resources, teamwork, employee commitment and concern for people. The respondents would prefer higher score on this dimension.

5.4.7 Overall organisational culture

Table 5.4.2 and Figure 5.4.7.1 show the overall score on organisational culture. Overall culture that dominants the study environment is hierarchy culture type where the work place is formalised and structured, heads of organisations view themselves as organisers and coordinators. Also, formal rules and policies hold the organisations together. Stability is a long-term concern where success is defined in terms of smooth scheduling and low cost. Moreover, the concern for management of employees is secure employment and predictability. Also, hierarchy culture is a preferred culture in the case study.

5.4.8 Conclusion

The results show that at the study environment overall the present organisational culture is hierarchy culture which scored 34.7%. Also, hierarchy culture is preferred by the respondents with the score of 36.8%. All the dimensions of organisational culture are dominated by hierarchy culture except the Criteria for Success and Management of Employees which are dominated by the Clan culture. According to Clan culture the Criteria for Success is express in terms of concern to people. In addition, Clan culture treats employees as members of extended family and a manager as parent figure. In Hierarchy culture Dominant Characteristics are express in terms of work place being formalised and structured; Organisational Leadership is viewed as coordinator and organisers; Organisational Glue is expressed in terms of rules and policies; and Strategic Emphasis is express in terms of stability and effectiveness.

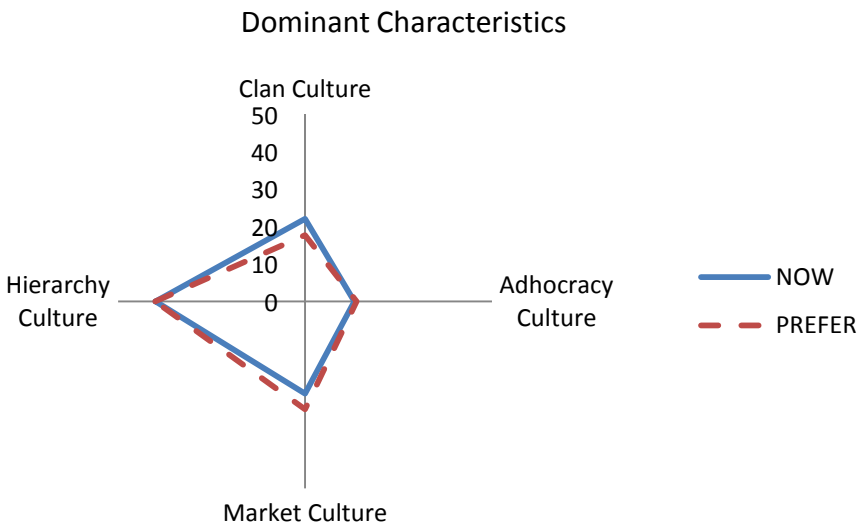

Figure 5.4.1: Dominant characteristics profile of Zanzibar public sector (45 respondents)

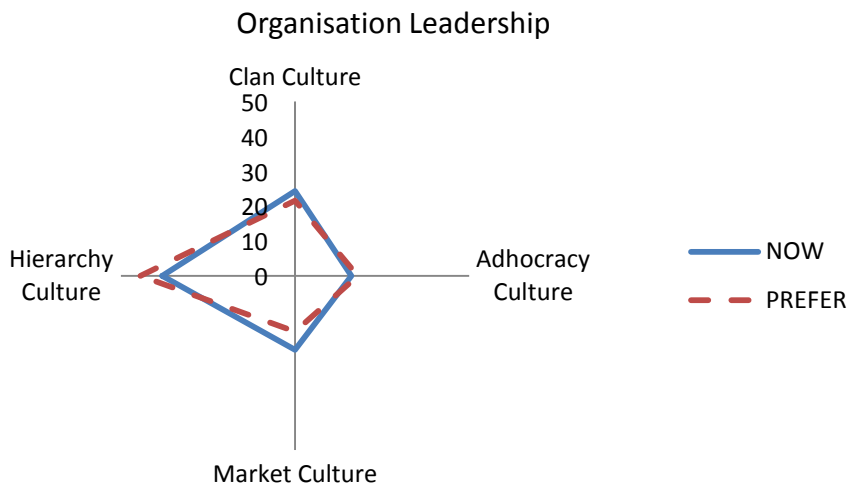

Figure 5.4.2: Organisational leadership profile of Zanzibar public sector (45 respondents)

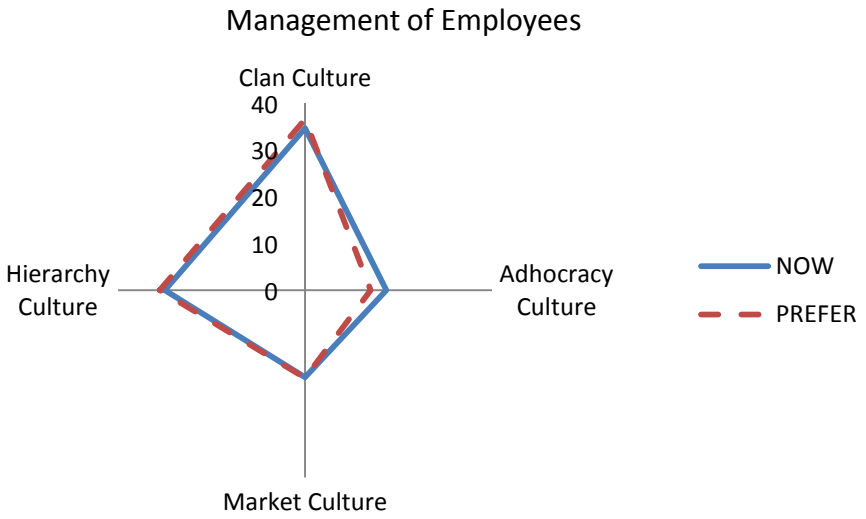

Figure 5.4.3: Management of employees' profile of Zanzibar public sector (45 respondents).

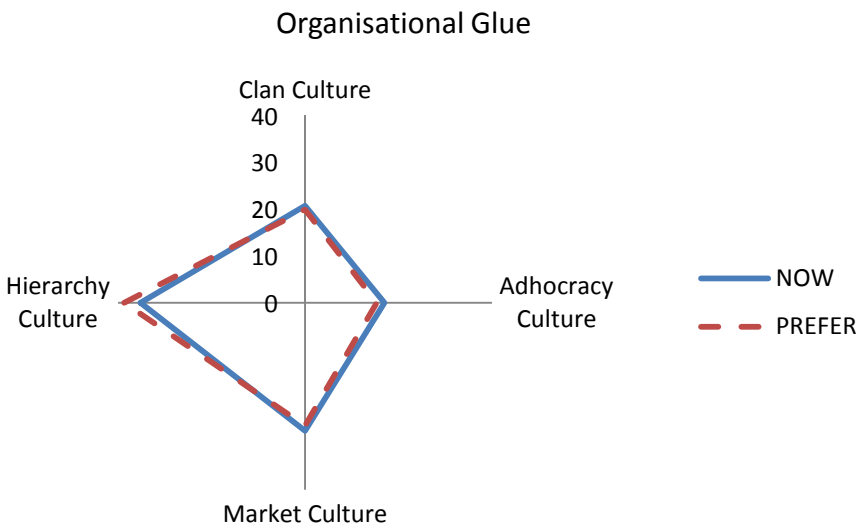

Figure 5.4.4: Organisational glue profile of Zanzibar public sector (45 respondents)

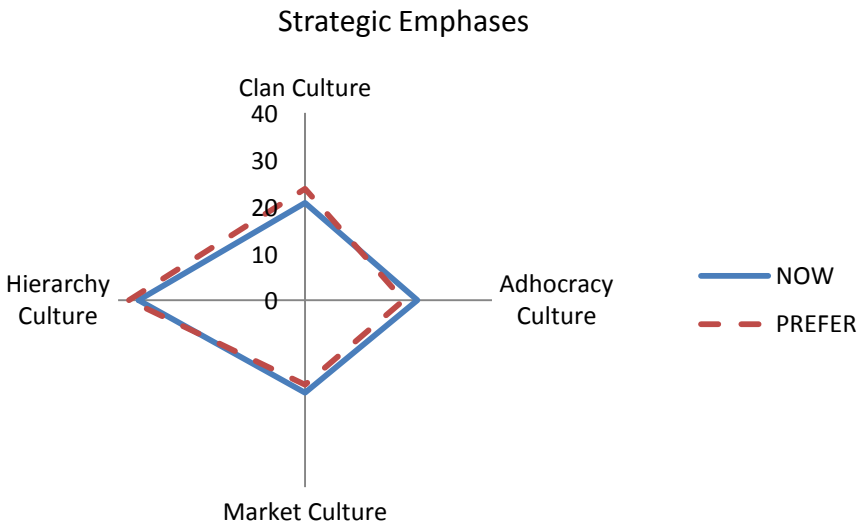

Figure 5.4.5: Strategic emphases profile for Zanzibar public sector (45 respondents)

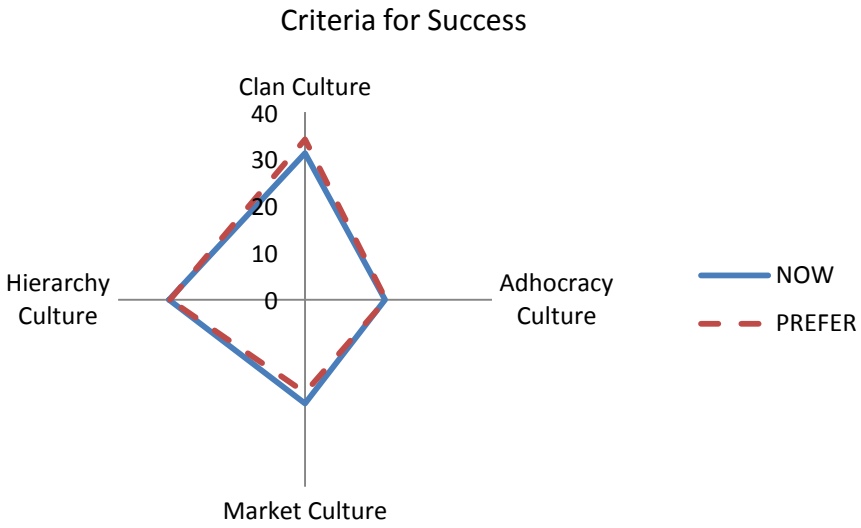

Figure 5.4.6: Criteria of success profile for Zanzibar public sector (45 respondents)

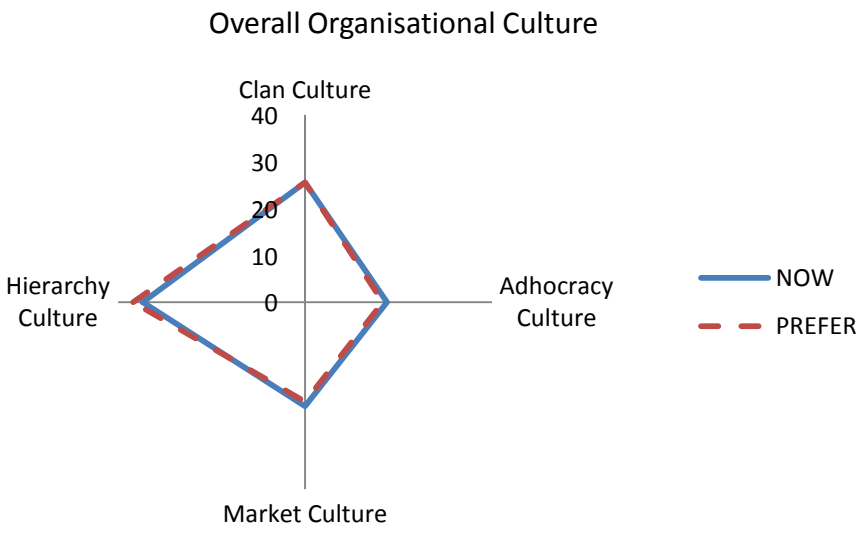

Figure 5.4.7: Overall organisation Cultural Profile (45 respondents)

Table 5.4.1: Results of each dimension of organisation culture (45 respondents)

Dimension	Culture Type	NOW (Mean)	PREFER (Mean)
Criteria of Success	Clan	31.3	34.3
	Adhocracy	17.1	17.3
	Market	22.2	19.9
	Hierarchy	29.1	28.9
Strategic Emphases	Clan	20.8	23.8
	Adhocracy	24	21.1
	Market	19.8	18.1
	Hierarchy	35.6	37.7
Organisational Glue	Clan	20.7	19.9
	Adhocracy	17	15.3
	Market	27.4	26.3
	Hierarchy	35.2	38.7
Management of Employees	Clan	34.7	36.6
	Adhocracy	17.4	14
	Market	18.6	18.7
	Hierarchy	30	31.1
Organisational Leadership	Clan	24.4	21.6
	Adhocracy	16.2	18
	Market	21.2	16
	Hierarchy	38.1	44.4
Dominant Characteristics	Clan	22	17.7
	Adhocracy	13.2	13.8
	Market	24.7	28.9
	Hierarchy	40	40.1

Table 5.4.2: Overall profile of organisational culture for Zanzibar public sector (45 respondents)

Culture Type	NOW	PREFER
Clan	25.6	25.6
Adhocracy	17.5	16.6
Market	22.3	21.3
Hierarchy	34.7	36.8

5.5 Cross Survey Analysis

This section presents the cross analysis of the surveys in sections 4.2, 5.2, 5.3 and 5.4 to identify correlation between information security practices and culture in the study environment.

5.5.1 Power distance

The results in section 5.3 show that the majority of respondents believe that power is shared unequally in the study environment, but they would prefer the power to be shared equally. In section 4.2.4 it was reported that many employees do not receive information security awareness training. Also, in Section 4.2.1 and 4.2.10 it was reported that information security policies and business continuity plans are not conveyed to employees. Respondent [DR1] said: "We do not have enough computers for everyone,

but XXX have their own laptops which they do not share, but other employees do share the computers.*"* Respondent [DR1] added: *"*When dealing with repairing computers belonging to bigwigs, I don't trust other employees to do the job, I do it myself." And respondent [DR14] commented: "There is bureaucracy and corruption in dealing with funds.*"* According to Carl, Gupta, and Javidan (2004, p.536) these findings are characteristics of a high Power Distance society.

5.5.2 Uncertainty avoidance

The results in Section 5.3.2 show that the majority of the respondents agreed that members of society both in practice and value seek orderliness, consistency, structure, formalised procedures, and laws to cover situations in their daily lives. In Section 4.2 it was reported that there is lack of documented information security policies, confidentiality or non-disclosure agreements, employment contracts which specifies terms that include information security, information security organs in the organisations, network operation guidelines, rules for using email and internet, data protection and privacy guidelines, business continuity plans and guideline for information system audit in the study environment. Also, many respondents feel that policies are not reviewed regularly. In addition, respondent [DR1] said:

> "There is a lot of hesitation in implementing policies. Employees are afraid of each other when implementing policies. They Fear of being label a bad or unkind boss. We have guidelines here that we try to implement but employees are not complying with them so we do not see the need to update them. Enforcement of disciplinary action is low. For example we do not have employees' attendance records."

And respondent [DR14] said: "There is a policy from the government which give priority to IT training but is not enforced here". Respondent [DR14] said:

> "We trust each other here because there are not many employees, this make us know each other. I can leave my computer without logging out. I can loan money to my fellow employee without signing a contract. Some bias is normal when dealing with trust base on nepotism or even people who hailed from same region."

Respondent [DR13] added: "We trust each other here, even we leave our phones in the office, and also I can leave my computer without logging out in my office". According to De Luque and Javidan (2004) these are characteristics of society with low Uncertainty Avoidance.

5.5.3 In-Group collectivism

The results in the section 5.3 show that the majority of the respondents agreed that both in practice and value this society takes pride in their families or organisations. Respondent [DR14] said:

> "We trust each other here because there are not many employees, this make us know each other. I can leave my computer without logging out. I can loan money to my fellow employee without signing a contract. Some bias is normal when dealing with trust base on nepotism or even people who hailed from same region."

Respondent [DR13] added:

> "We trust each other here, even we leave our phones in the office, and also I can leave my computer without logging out in my office."

Respondent [DR12] added:

> "Enforcement of policies is very weak here especially those involving finance are difficulty to be implemented. There is bias in implementing policies among groups of people who works here especially those who hailed from same district."

Respondent [DR3] said:

> "There is no bias in implementing policies in the last six months but before that there was bias based on political interest although they were done in the secrecy."

The results show that there are employees who allowed a relative to use their organisations' computers. Also, there are employees who shared a password with someone else. According to Gelfand at al. (2004, p.454) these findings are characteristics of a society with high In-Group Collectivism.

5.5.4 Future orientation

The results in the section 5.3 show that the majority of respondents agreed that in the study environment people are not planning for the future. However, the majority of respondents prefer to plan for the future. In the study organisations we note that none had information security strategy. Also, in section 4.2.10 it was reported that there is lack of Business Continuity Plans in many organisations in the study environment. We noted in Section 4.2.2 that information security has not been integrated into corporate governance in many of studied organisations. Also, there are no qualified professional information security employees in the study environment. In addition, there are no guidelines for

quantifying and monitor information security incidents. According to Ashkanasy et al. (2004, p.302) these are characteristics of a society with a low Future Orientation.

5.5.5 Organisation culture

The results in the section 5.4 show that the overall organisation culture that dominants public organisations in Zanzibar is hierarchy culture type where the work place is formalised and structured, heads of organisations view themselves as organisers and coordinators. Also, formal rules and policies hold the organisations together. Stability is a long-term concern where success is defined in terms of smooth scheduling and low cost. Moreover, the concern for management of employees is secure employment and predictability.

The results in Section 4.2.2 show that the majority of respondents did disagree or were undecided that there is a budget for information security program. Also, the majority of the respondents disagreed that their organisations are capable of implementing information security awareness programs. And, in Section 4.2.4 it was reported that there are lacks of regular training on information security awareness in the study organisations. Respondent [DR2] said: "Funds availability is very poor; sometimes we only get funds for 10% of the budget". Respondent [DR15] said: "There are problems in getting funds for implementing our daily tasks. If we want to aim high funds are not available". This shows that the study organisations avoid costly activities. According to Cameron and Quinn (2006) in a hierarchy culture, success is defined in terms of low cost.

5.6 Discussion on research findings

Findings suggested that in the case study power is shared unequally; there is no orderliness, consistency, structure and laws to cover daily lives; there is in-group collectivism; and society is not future oriented. These findings suggested that these societal issues affected the effectiveness of information security in the case study.

Power distance is the one of the reason of inequality in level of security in the organisations in the case study. Organisations that provide services involve finance, voting and citizen registration are viewed as important hence their security is higher than others. New policies are not communicated to employees and there is unequal distribution of IT equipment. If policies are not communicated there could be compromise of the IT systems in the organisation. An employee who is not aware of policy for downloading software into organisation's computer could spread virus into the organisation. As reported in chapter 4, 80% of study organisations suffered virus attacks. Lack of IT

equipment in certain areas of an organisation may compromise the security of the whole organisation. Installing anti-virus to the organisation's bigwigs alone could create a virus scare to other systems in the organisation. Findings in this study suggested that in the case study there is lack of skilled information security professionals. Findings in the literature suggested that unequal sharing of power causes corruption, few employees have access to resources; few skilled employees; information is not shared and low human development (Carl, Gupta and Javidan; 2004).

Uncertainty Avoidance influences the information security as we have shown that the study environment does not seek orderliness, consistency, structure, formalised procedures, and laws to cover situations in their daily lives. This has been shown due to lack of policies, laws, guidelines, and procedures that govern information security in the study environment. When policies are not reviewed they jeopardise the IT systems to new threats. Laws, policies, guidelines and procedures deter humans from committing acts that could compromise the IT infrastructures. Findings show that contracts signed by employees did not include information security. Findings suggested that employees broke rules without being punished. Findings in literature suggested that society with lower uncertainty avoidance tends to be informal; tolerate to break of rules; rely on trust and less likely to establish rules (De Luque and Javidan, 2004).

In-Group Collectivism did influence the information security governance in the case study. The study environment believes in taking pride in their families or organisation. This may compromise the IT infrastructure especially sensitive information that is needed by a political group. Findings suggested that employees were ready to break rules in order to allow their relative access to equipment; employees shared their passwords. In literature it is suggested that society that take pride in their family or organisation, employees tend to value group activities more (Gelfand at al., 2004).

Future orientation has influenced the information security governance as we have shown that the study environment does not plan for the future. Information security is still not part of corporate governance in the study environment. Also, there is a lack of business continuity plans, lack of guidelines for monitoring information security incidents and lack of training strategy for employees.

Furthermore, findings suggested that organisations in the case study are dominated by hierarchy culture. The findings are consistent with findings in the literature on public organisation (OCAI, 2010). Findings suggested that hierarchy culture has minor influence

on effectiveness of information security governance. As mentioned in the section 2.6.2, in hierarchy culture procedures control what employees do. But, findings in the chapter 4 suggested that information security governance in the case study implement ad hoc practices. Hierarchy culture is one of the reasons for lack of funds for information security project in the case study.

5.7 Conclusion of findings

The investigation provided a wide range of views on understanding the complex societal issues that influence the management of information security in the context of Zanzibar.

Overall, the analysis of the study environment in section 5.3 revealed that in the study environment power is shared unequally. There are a significant number of members of society who do not seek orderliness, consistency, structure, formalised procedures, and laws to cover situations in their daily lives. Society is not humane orientated; rewards collective distribution of resources; takes pride in their family or organisations; has significant element of assertiveness and confrontation; has gender inequality; is not planning for the future; and rewards members for performance progression and brilliance. In addition, the findings show that the overall organisation culture is hierarchy.

The cross analysis in section 5.5 demonstrated that some cultural dimensions have influenced the state of information security in the study environment. National culture dimensions that impact the management of information security appeared to be future orientation, power distance, in-group collectivism and uncertainty avoidance. Organisation culture dimensions appeared to have little impact on governance of information security. All the dimensions are dominated by hierarchy culture except the criteria for success dimension which is dominated by the clan culture. In a hierarchy culture, an organisation is "a very formalised and structured place to work. Procedures govern what people do" (Cameron and Quinn; 2006, p.66). In this culture the dimension that influenced information security is criteria for success. In this dimension has influenced information security by controlling availability of funds. Public sector has rules and procedures adapted from colonial ruler. Information security governance is new area that did not exist during that time. This explains why information security governance is in ad hoc practices.

The next chapter, Chapter 6, will provide a framework for information security culture.

Table 5.6.1: Overview of study findings

Data Construct	**Findings**
Power Distance	Power is shared unequal in Zanzibar and affects the governance of information security.
Uncertainty Avoidance	Society does not seek orderliness or laws to cover daily lives and affect the governance of information security.
In-group Collectivism	Society in Zanzibar takes pride in their family or organisation and affects the governance of information security.
Future orientation	Society in Zanzibar does not plan for the future and affects the governance of information security.
Institution Collectivism	Society in Zanzibar rewards collective distribution of resources but does not affect information security governance.
Gender Egalitarianism	There is gender inequality in Zanzibar but does not affect the governance of information security.
Human Orientation	Society in Zanzibar is not caring or kind but does not affect the governance of information security.
Assertiveness	Society in Zanzibar is not confrontational but does not affect the governance of information security.
Performance Orientation	Progression and brilliance is rewarded in Zanzibar but does not affect the governance of information security.
Organisational Culture	The overall culture is hierarchy with little impact on information security governance.

CHAPTER 6

6 A FRAMEWORK FOR INFORMATION SECURITY CULTURE

6.1 Introduction

This chapter presents a framework for information security culture in non-profit organisations in the context of Zanzibar. The main objective of this research is to improve the quality of information security governance in non-profit organisations in the context of Zanzibar. The study investigated information security governance, and cultural factors that influenced the management of information security. The findings in Chapter 4 and 5 together with literature reviewed in Chapter 2 are used to recommend a framework for information security culture in non-profit organisations. The framework helped to answer the research question RQ4.

6.2 Proposed framework for information security culture

In Figure 6.3.1, a framework for information security culture in the context of Zanzibar for non-profit organisations is proposed, developed from the two phases of the study as presented in Section 4.2, 5.2, 5.3 and 5.4. In this section, the individual elements of the framework are discussed in detail.

6.2.1 National culture

The findings in Section 5.2, 5.3 and 5.5 were used for recommendation of this framework. National cultures influence the governance of information security in the context of Zanzibar and should be considered in the developing of information security culture. Organisations should be aware of dimensions of national culture that could jeopardise the information security. Appropriate policies should be developed to control

threats caused by national culture influenced behaviour. Training and awareness should be provided to employees on acceptable good behaviour for information security culture. Organisations should start sharing power policy by introducing transparency and employees' participation in decision making. Organisations should find the way to raise the salary of their employees. Organisations should be aware of culture of loyalty to a group or family by their employees. Organisations should provide awareness training to their employees on law enforcement process and work planning.

6.2.2 Organisational culture

The findings in Section 5.4 and 5.5 were used for recommendation in this framework. Organisational culture influences the governance of information security. Organisations should ensure availability of funds for an information security program. This could be achieved by making information security as part of corporate governance of non-profit organisations. This will enable information security to be monitored by top management and various policies and guidelines developed for information security. Also, top management will ensure policies are enforced and reviewed in a regular basis. Non-profit organisations could establish information security committees in the organisations to monitor information security governance. Non-profit organisations should develop and test business sustainability plans to ensure continuity. Organisations should ensure that their employees are in compliance with national laws and organisation's policies. Organisations should ensure that any non-compliance is reported to police or activates a disciplinary action.

6.2.3 Government responsibility

The findings in Section 4.2 and 5.2 were used for recommendation for this section. Government has an important role to play in ensuring good information security culture is achieved. Government has a duty to establish and enforce laws, regulations, strategies and policies for protecting information. In addition, the government has a duty to ensure organisations have well trained employees. This could be done through establishing education and skills training for information security at higher education institutions. Government should establish awareness program for information security for all. Public owned radio station, television station and newspapers can be used in providing information security awareness. The Ministry of Education and Vocational Training can help to ensure this program is established in the context of Zanzibar. Government should ensure availability and distribution of resources for information security program.

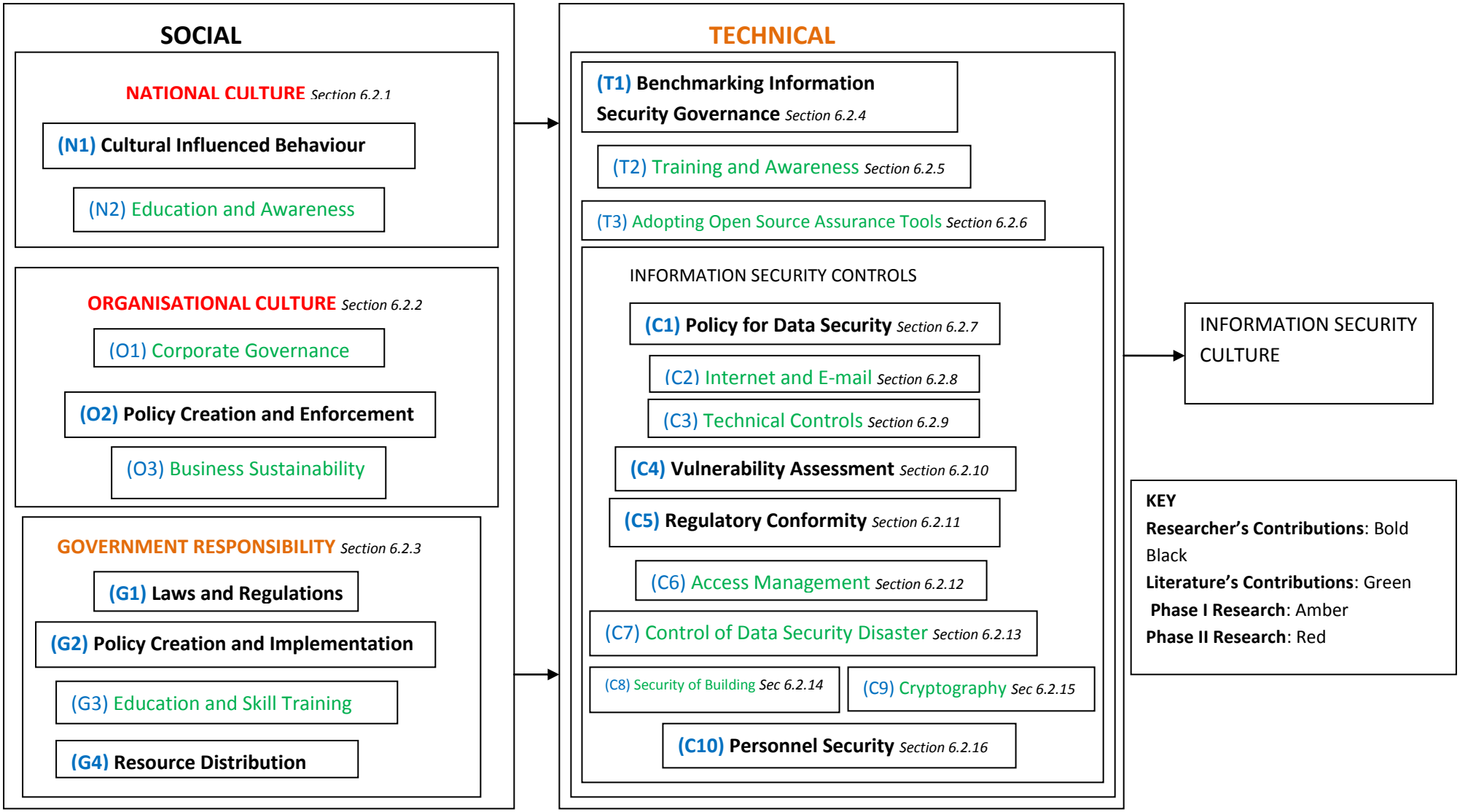

Figure 6.3.1: Proposed Framework for Information Security Culture

Various governmental strategies are available in the literature (NISC, 2010; NISS, 2007; Cabinet Office, 2009; ITU, 2005) and were discussed in detail in Section 2.5. Legislation should be strengthened in areas such as content filtering, protection of children online, digital evidence, digital signature, electronic document and privacy. The government should ensure that there is strong law enforcement and due process. The government should establish Computer Emergency Response Team which will be responsible for handling information security incidents. Activities of this team could be monitored by one of government ministries. In the context of Zanzibar, this could be done by the Ministry of Communications and Transportation. The statute (Zanzibar, *Public Service Act* 2010) should be reviewed to add terms and conditions of employment that specify information security. Also, the review should include third party and contractor accessing organisations. Finally, the Government must take responsibility to ensure non-profit organisations implement a benchmarking policy on information security. The government should seek help from the United Nations and other development partners in accomplishing this objective.

6.2.4 Benchmarking of information security governance

The findings in Sections 4.2 were used for recommendation in this framework. Information security practices in organisations must be benchmarked to the appropriate international standards. Organisations should train their employees to be able to implement adapted standards and best practices based on their organisations' requirements. Care must be taken on the controls that could be affected by national cultural behaviour. Top management must provide support to the benchmarking process in the form of budgets, training of existing employees and hiring skilled information security personnel.

6.2.5 Training and awareness

The findings in Section 4.2 were used for recommendation in this framework. Training and awareness are essential for developing desired information security culture in an organisation. Organisations should conduct training and awareness in information security regularly. Web-based training and awareness are cost-effective and improve security awareness level (Shaw et al, 2009; Whelan and Wright; 1999). Web-based training is available all times which facilitates the training of employees. Emails and wall posters can be used in raising information security awareness in an organisation. NIST (1998) can be used to benchmark information security awareness training in an

organisation. For example, the game Anti-phishing Phil is a web-based security awareness game that raises awareness on phishing attacks (Sheng et al, 2007).

6.2.6 Adopting open source assurance tools

The findings in Section 4.2 and 5.2 were used for recommendation in this framework. According to OSI (2012) Open Source Software is the software whose source code is available to the public and it can be used, modified and redistributed along with the original rights as described by Open Source Initiative (OSI). An open source software is inexpensive and save development time (Nishimura and Sato; 2009). There are many open source frameworks available in the literatures that provide information assurance. The on-the-fly encryption software is open source software used for creating and retaining an on-the-fly-encrypted volume where data is automatically encrypted right from before it is saved and decrypted right after it is loaded (Truecrypt, 2012). The Password Complexity Filter is an open source software developed using Perl that is made freely available under Perl artistic license and is designed to illustrate various ways in which organizations can integrate password complexity checks into their internally developed applications, in particular applications that are network or cloud based (In Silico Biotechnologies, 2012). The Password Complexity Filter can be customised to concur with organisational password policies. The Zimbra Collaboration Suite (ZCS) open source edition is a fully-fledged application consisting of messaging and collaborative solutions that include emails, address book, calendaring, tasks, and Web document authoring (Zimbra, 2012a). It is designed to offer an end-to-end mail solution that is scalable and reliable. The suite has been bundled with Clam Anti-Virus and SpamAssassin software (Zimbra, 2013b). Clam Anti-Virus provides virus protection by putting in quarantine messages that contain viruses. The life time for these messages is 7 days. SpamAssassin provides a filter for unsolicited commercial emails with learned data stored in either the Berkeley DB database or MySQL database. Predefined rules as well as Bayes database are utilised in SpamAssassin to score messages (Zimbra, 2013b). The score is used to determine whether a message is spam or not. Port scanner is software that is used to investigate exploits at ports (transport layer). Port scanner can be used for investigating network inventory, network optimization, finding spyware, Trojan horses and worms; and looking for unauthorised or illicit services (Howlett, 2005). NMAP is an open source version of port scanner (Insecure.org, 2012). Vulnerability scanner is software that is used to find security holes in applications on the information system that are exploitable. Source of vulnerabilities could be buffer overflows, router or firewall weaknesses, web server weaknesses, mail server holes, DNS servers, databases

weaknesses, user and file system; default accounts, blank or weak passwords; unwanted services; leakage of information among others (Howlett, 2005). NESSUS is an open source software version of vulnerability scanner (Tenable Network Security, 2013). Network intrusion detection system is used to listen to packets at the physical layer. Tcpdump is an open source software version of an intrusion detection system which comes with Linux distribution. Snort is an open source software version of intrusion detection system and intrusion prevention system (Snort, 2013). Logfiles can be analysed for security vulnerabilities using open source software called Swatch (SWATCH, 2013). Training will be needed to technical staff in order to implement these tools.

6.2.7 Policy for data security

The findings in Section 4.2, 5.2, 5.3 and 5.5 were used for the recommendation in this framework. Organisations must establish a data security policy. The policy must be communicated to employees, reviewed regularly and documented. Employees must comply with the policy and any non-compliance must activate disciplinary actions. Organisations should ensure cultural behaviours such as corruption, nepotism, political party affiliation and religious extremism are countered for effective enforcement of policies.

6.2.8 Internet and e-mail

The findings in the Section 4.2.6 and 5.2 were used for recommendation in this framework. Organisations must establish a policy for internet usage and e-mail communications. Non-compliance of this policy must activate disciplinary actions. Organisations should encourage the implementation of e-mail server with encryption capabilities. Organisation should install filters to protect internet users from obscene materials. DansGurdian is an example of open source web content filtering software which can be adapted to the needs of an organisation (Dansguardian, 2013).

6.2.9 Technical controls

The findings in Section 4.2.6, 4.2.7, 4.2.8, and 4.2.12 were used for recommendation in this framework. Organisations should establish procedures, guidelines and policies on technical controls according to their requirements. Technical controls including but not limited to software back-up, network operations, system auditing, system acceptability, user logs, web hosting, exception handling, and removal of media. Organisations should introduce the implementation of intrusion detection/prevention systems. Also, should

establish a policy on the use of unauthorised software. Benchmarking of information security process and training of employees for skills is very important in this part.

6.2.10 Vulnerability assessment

The findings in Section 4.2.8 were used for recommendation in this framework. Organisations must conduct vulnerability assessments to all systems regularly. Organisations must provide skills training to technical staff so that they can carry out the assessments. Open source software such as NESSUS should be recommended for use in vulnerability assessment.

6.2.11 Regulatory conformity

The findings in Section 4.2.11, 4.2.12, 5.2 and 5.5 were used for recommendation in this framework. Organisations must ensure that their employees comply with the country's laws and regulations. Organisations should ensure that their employees comply with policies of their organisations. Organisations have to ensure that their organisations are in compliance with all technical requirements according to their systems. Organisations should audit their information systems regularly. Organisations should develop a strategy to deal with cultural influenced non-compliance behaviours such as corruption, nepotism, political party affiliation and religious extremism.

6.2.12 Access management

The findings in Section 4.2.7, 5.2 and 5.5 were used for recommendation in this framework. Organisations must establish access control policy. Organisations must provide every employee with unique access to information systems. Organisations must record all shared access to information systems. Organisations should make full use of authentication mechanisms provided by operating systems such as Active Directory Domain Services for Windows operating system; and Lightweight Directory Access Protocol (LDAP) and Kerberos for Linux operating system. Organisations should encourage the use of biometric authentication.

6.2.13 Control of data security disaster

The findings in Section 4.2.9 were used for recommendation in this framework. Organisations should record and financially quantify all security incidents. Organisations must provide awareness to employees about reporting security incidents. Organisations must have clear policies on reporting security incidents.

6.2.14 Security of building

The finding in Section 4.2.5 and 5.2 were used for recommendation in this framework. Organisations must provide IT literacy training to building security employees. Building security employees must be integrated into information security department. Organisations must physically lock their computers. Organisations must record and check the identity of visitors in their premises. Organisations must enforce policy for employees to wear identification cards. Organisations should install electronic locks at their premises. Armed security guards should be provided to organisations that have critical information assets. Organisations should establish and enforce a policy on equipment handed to employees.

6.2.15 Cryptography

The findings in Section 4.2.7, 4.2.8, 5.2 and 5.4 were used for recommendation in this framework. Organisations should establish policy on adopting cryptographic technology for their operations. Technical staff must be trained in cryptographic technology skills. Organisations must provide awareness on the use of encryption to employees.

6.2.16 Personnel security

The findings in Section 4.2.4, Organisations must ensure employees' backgrounds are checked. Organisations must review their employment contracts to include terms that reflect information security. Organisations must ensure that employees are provided with information security expectation of their roles. Organisations must establish policies that will protect organisations from cultural behaviours that endanger the security of organisations. Information security awareness training should be provided in a regular basis to all employees. Posters should be used to provide employees with awareness on laws and policy on information security.

6.3 Conclusion

This chapter began with the discussion of the findings in the study. Next a detailed explanation of the proposed framework of information security culture for non-profit organisations in the context of Zanzibar was provided. This framework was developed by considering social and technical issues facing the case study. The researcher's contributions for this thesis are found in Section 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.7, 6.2.10, 6.2.11, and 6.2.16. Section 6.2.5, 6.2.6, 6.2.8, 6.2.9, 6.2.12, 6.2.13, 6.2.14 and 6.2.15 are found in the literature. See Figure 6.3.1 for details.

The next chapter, Chapter 7, discusses a process model for improving information security governance in non-profit organisations that evaluated the proposed information security cultural framework.

CHAPTER 7

7 EVALUATION OF THE FRAMEWORK FOR INFORMATION SECURITY CULTURE USING SEMIOTICS

7.1 Introduction

This chapter evaluates the framework for information security culture in non-profit organisations in the context of Zanzibar using techniques adapted from the organisational semiotics. A process model for information security governance will be developed in order to evaluate the framework proposed in Chapter 6. This model is grounded by the theory of semiotics. It integrates social and technical issues in order to enhance information security governance. A brief literature review on organisational semiotics was presented in Section 2.8. This chapter builds on this by developing a semiotic process model. This model uses the issues identified in Chapter 6 as well as the data collected in Phase I and Phase II of the research (Chapter 4 and 5) as a point of reference and in doing so evaluates the framework for information security culture in Figure 6.3.1. The framework helped to answer the research question RQ4 and the main research question RQM.

7.2 Semiotics framework

Semiotics is a study of signs in which a sign represents something to someone for something else (Liu, 2000). According to Gottdiener (1995), a sign is composed of expression and content. Signs are tools that facilitate social interactions (Gottdiener, 1995). A sign is a medium for human to understand things. People communicate significance, create meanings, and convey thoughts and sentiments via signs or sign systems. Signs and norms cannot be separate (Stamper et al., 2000) and work together. Culture or subculture

is defined by shared norms. Therefore, the notion of culture is an important aspect within organisational semiotics. Organisational semiotics provides approaches, frameworks, and methods to both analyse and design organisations (Liu, 2000; Stamper et al, 2000). "Organisational semiotics defines an organisation as a social system or a social structure in which people behave in an organised manner by conforming to a certain system of social norms" (Rambo, Liu and Nakata; 2009). Culture is formed by shared norms. In Zanzibar, it is a norm to help a relative even if it involves breaking the law.

Stamper et al (2000) divided signs into six layers that have their own layers of norms. These layers are social world, pragmatics, semantics, syntactics, empirics and physical world. These six layers of signs collectively are called semiotic ladder or semiotic framework (Liu, 2000). These layers then allow the analysis of any information system depth. Figure 7.2.1 shows the semiotic framework for analysing information systems. We will discuss the layers of semiotic framework in the following sub-sections. In this chapter, the semiotic framework is applied to analyse and design the process model.

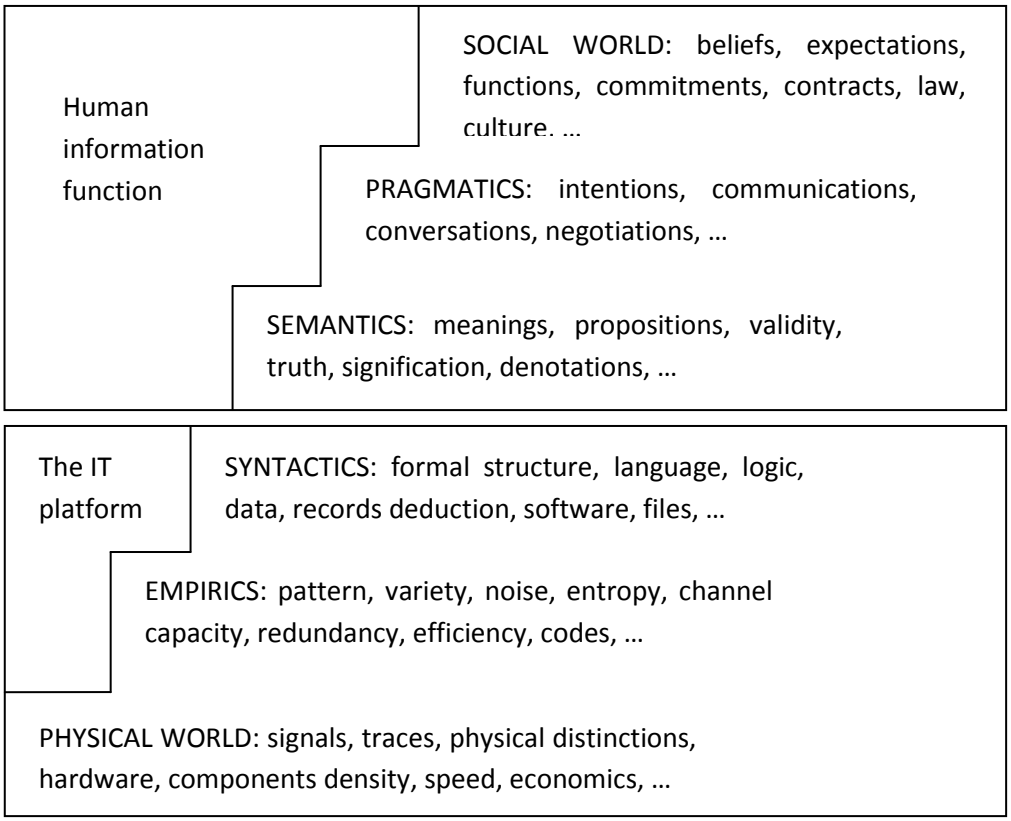

Figure 7.2.1: The semiotic framework (Adopted from (Liu, 2000))

7.2.1 Social world

The social world layer presents analysis and design requirements that influence the social world of the information technology user. The analysis works on the effects or outcomes of pragmatic communication. That is, when a meaningful declaration has arisen, the social layer is employed to discover the social norms that would be transformed, changed, or influenced in some way. Some of the examples of these social norms might include beliefs, expectations, functions, commitment, contract, law, and culture. Here is where social norms that influence culture are interpreted by individuals. Liu (2000) categorised norms as follows:

- Perceptual – accepted ways of viewing the world
- Cognitive – measured beliefs and knowledge possessed by a community
- Evaluative – guide the community towards common courses
- Behavioural – control members so that they behave in a correct manner

The culture of the organisation is important because signs are used upon the culture in which they belong.

7.2.2 Pragmatics

According to the semiotic framework here is found intentions, communications, conversations, and negotiations. Here is where one can understand the purpose and relationship among cultural behaviours. Organisations with pragmatic problems are in a state of confusion (Liu, 2000). Communication is considered successful if a message is passed by a sender is interpreted by a receiver as intended by the sender. Here is where one can understand the purpose and relationship among cultural behaviours.

7.2.3 Semantics

In the view of the semiotic framework here is found meaning, propositions, validity, truth, signification, and denotations. Here is where one can understand the meaning of cultural behaviour. Employees from different backgrounds need to understand each other in order to work together. Semantic problems that an organisation may encounter are a new market notion, new technology, and a new organisational notion among others (Liu, 2000).

7.2.4 Syntactic

In the opinion of the semiotic framework here is found formal structure, language, logic, data, records deduction, software, and files. Here is where one can compose cultural behaviour from simple behaviours. Culture can be coded following a certain design. In an

organisational environment activities are often in disorder and issues of interest is how to bring order and structure in the organisation (Liu, 2000).

7.2.5 Empirics

On the empirical level culture meets technology. Physical phenomena are organised into predictable and recognised patterns. In an organisation events are loaded with randomness. Business matters are managed in uncertainty (Liu, 2000). According to semiotic framework here is found pattern, variety, noise, entropy, channel capacity, redundancy, efficiency, and codes.

7.2.6 Physical world

Here is where the culture meets the hardware. Physical issues deal with the media for storing and transporting signals. Business issues occur due to the economics of the physical resources. According to the semiotic framework here is found signals, traces, physical distinctions, hardware, component density, speed, and economics.

7.3 Mapping between semiotic framework and national cultural dimensions

As mentioned in the section 3.4.2, this research has adopted national cultural dimensions derived from the GLOBE Project. The descriptions of the dimensions were provided in section 2.7.1. Table 7.3.1 shows the mapping between organisational semiotics to cultural dimensions. In this research, cultural dimensions represent semiotic of culture. The purpose of this table is to show how each layer is influenced by the national culture. Social world, pragmatics and semantics levels are influenced by all the dimensions of culture. However, the layers of Syntactics, Empirics, physical world are influenced by power distance, uncertainty avoidance, future orientation and performance orientation only. Also, the physical world is influenced by in-group collectivism and humane orientation. Every society will have different cultural dimensions affecting their information security governance. In Zanzibar, for example, it is a norm for an employee to allow a relative to access internet through the employee organisation's computer. The impact of culture on semiotic layer could be high, medium, low or not there at all as shown in the Table 7.3.1.

Table 7.3.1: Mapping between organisational semiotics and cultural dimensions.

	SEMIOTICS LAYERS					
CULTURAL DIMENSIONS	**Social World**	**Pragmatics**	**Semantics**	**Syntactics**	**Empirics**	**Physical World**
Power Distance	High	High	High	High	Low	Medium
In-Group Collectivism	High	High	High	Not there	Not there	Low
Uncertainty Avoidance	High	High	High	High	Low	Medium
Gender Egalitarianism	Medium	Low	Low	Not there	Not there	Not there
Future Orientation	High	Medium	Medium	High	Medium	Low
Institution Collectivism	High	High	High	Not there	Not there	Not there
Performance Orientation	Low	Low	Low	High	High	High
Assertiveness	Low	Low	Low	Not there	Not there	Not there
Humane Orientation	Low	Low	Low	Not there	Not there	Low

7.4 Towards a semiotics process model

The term 'process' here denotes a set of interrelated activities, which transforms inputs into outputs as defined in ISO/IEC 15504 (2004). According to Unified Modelling Language (UML) a model is a simplification of reality. Therefore, a model might be an equation, a diagram, a physical model, a piece of text or any verbal description. A process can be written down to take a form such as a standard, a procedure, a set of guidelines or work instructions. An international standard is a very high-level process while guidelines and work instructions are very low-level processes (Holt, 2005). Table 7.4.1 shows the proposed semiotic framework for analysing information security governance in the organisation. From the discussions in the section 7.2, and mapping in the section 7.3, a semiotic diagnostic framework for information security governance is proposed in the Table 7.4.1. The description of each layer of the semiotic diagnostic is provided in the following sub-sections.

7.4.1 Social world

In the perspective of information security, social world analysis necessitates that the dedication of the organisation is expressed and supported with a feasible information security strategy. Analysis of national culture dimensions that impact this layer can be done here. The analysis of information security policy, legal framework, employee's contract, corporate governance, education, training and awareness belong to this layer.

7.4.2 Pragmatics

In the context of information security communication and negotiation, it is important at various level of an organisation in order to implement security strategy. Issues at this level have to be resolved at the highest level in the strategic planning and micro-level in the design of information security strategy. Analysis of email policy, encryption policy, network policy, access control policy, a national culture dimensions that influence this layer should be done here.

Table 7.4.1: A semiotic diagnosis for information security governance design requirement (Adapted from: Liu, 2000; ISO/IEC 27002)

Semiotics Layer	Information Security Issues
Social World	Information security strategy, information security policy, legal compliance, information security standards and best practices; education, training and awareness; employment contract, corporate governance, national culture dimensions that influence security
Pragmatics	Email policy, encryption policy, network policy, access control policy, leakage of confidential information, national culture dimensions that influence this layer
Semantics	Review of policies, testing of business continuity plan, screening of employees, assigning role and responsibilities, reviewing access rights, national culture dimensions that influence this layer
Syntactics	Penetration test, virus protection, data backup, data encryption, intrusion detection, firewall, file permission, authentication, software usage, auditing of systems, national culture dimensions that influence this layer
Empirics	Internet bandwidth, recording of security breaches, national culture dimensions that influence this layer.
Physical World	Penetration of hardware in the organisation, physical security, and national culture dimensions that influence this layer.

7.4.3 Semantics

In the perspective of information security, semantic layer analysis necessitates that senses and outcomes of various security design problems be examined. Through this kind of analysis, problems such as the outcomes of misinterpreting data or misuse of regulations are determined that leads to the creation of accountability structures. Review of policies, auditing of systems, testing of business continuity plan, screening of employees, assigning role and responsibilities, reviewing access rights, national culture dimensions that influence this layer should be analysed in this layer.

7.4.4 Syntactic

In the perspective of information security, the analysis of the syntactic layer entails that the appropriate processes such as penetration test, virus protection, data backup, data encryption, intrusion detection, firewall, file permission, authentication, and national culture dimensions that influence this layer to be analysed.

7.4.5 Empirics

In the perspective of information security, the empirics' layer analysis necessitates that suitable telecommunication equipment and network strategies to be determined to correctly handle the security requirements of an organisation. In Addition, internet bandwidth, recording of security breaches and national culture dimensions that influence this layer can be analysed here.

7.4.6 Physical world

In the perspective of information security, physical world analysis necessitates that the suitable hardware to be determined to offer both precise information and physical security of assets. Penetration of hardware in the organisation should be considered here. Additionally, national culture dimensions that influence each layer should be analysed at this layer.

In the next section, semiotic diagnostic framework will be implemented to develop the process model for information security governance in non-profit organisations.

7.5 Proposed semiotic process model

The findings in the chapters 4 and 5 are used to develop the process model presented in Table 7.5.1.

7.5.1 Analysis of the social world layer

Table 7.5.1 presents the analysis and solutions of the findings in Chapter 4 and Chapter 5 grounded by the social world analysis. We can group the problems into skill, culture, and corporate governance. In the skill group, there is lack of qualified information security experts and lack of training and awareness in information security. In the culture group, there are several issues here. The issues are the existing policies are not communicated to employees; issues of corruption; employees not signing confidentiality agreements; not including information security clause into the employment contract; and lack of benchmarks in information security management. In the corporate governance group, there are two issues which are a lack of strategy for integrating information security into corporate governance and a lack of budgets for a thorough and relevant information security program.

Table 7.5.1: Proposed Semiotic Process Model

Semiotic Layer	**Issues Faced (INPUT)**	**Solution (OUTPUT)**
Social World	Lack of qualified information security professionals and lack of regular information security training and awareness.	Education, Training and Awareness Policy
	Information security policy not conveyed to employees.	Education, Training and Awareness Policy
	Lack of benchmarks in information security management.	Standards and Best Practices Adaption Policy
	Issues of favouritism and corruption.	Compliance Policy
	Employees are not signing confidentiality agreements and terms of employment lack information security item.	Employee Security Policy
	Lack of budgets for information security program.	Corporate Governance
Pragmatics	Lack of policy for email, internet usage, network service and encryption.	Communication and Web Policy
	Lack of documentation for security features, service levels, and management requirements of all network services	Documentation Policy
	Issues of employees sharing passwords and lack of systems to manage password.	Access Control Policy
	Issues of employees leaking confidential information to their affiliated political parties.	Confidential Information Policy
Semantics	Information security policies are not reviewed regularly	Review and Evaluation Policy
	Business continuity plans are not tested	Business Continuity Policy
	Employees' backgrounds are not checked	Employees Security Policy
	Employees unaware of information security expectations of their positions	Employees Security Policy
Syntactics	Lack of policy for use of unauthorised software	Use of Unauthorised Software Policy
	Lack of guidelines for acceptance of new systems	New Systems Acceptance Policy
	Lack of intrusion detection systems	Assurance Policy
	Lack of assessment for security vulnerabilities	Vulnerability Assessment Policy
	Lack of guidelines for systems audit	Systems Auditing Policy
Empirics	Lack of guidelines for recording and quantifying security breaches	Security Incidence Policy
	Internet bandwidth is very limited and expensive	Corporate Governance
Physical World	Security guards are illiterate and cannot use IT equipment	Education, training and awareness Policy
	Fewer employees have access to computers	Corporate Governance
	Employees allow relatives to use computers belong to their organisation	Employees Security Policy
	Computers are not physically locked	Equipment Policy

7.5.2 Analysis of pragmatic layer

As shown in Table 7.5.1, the case study presented several issues that needed an initial examination at the pragmatics layer. The problems can be grouped into two, technical and culture. The technical problems were that the lack of policies for email and internet usage, use of network services, and encryption. Also, there is a lack of systems to manage passwords, lack of guidelines for network operations, and lack of documentation for security features, service levels, and management requirements of all network services. The cultural problems are employees sharing their password and leakage of confidential information to political parties.

7.5.3 Analysis of semantic layer

As shown in Table 7.5.1, the case study presented several issues that needed an initial examination at the semantic layer. The problems are all cultural in nature. They are: not reviewing information security policies; business continuity plans are not tested; employees' backgrounds are not checked; and employees unaware of information security expectations of their positions.

7.5.4 Analysis of syntactic layer

As shown in Table 7.5.1, the case study presented several issues that needed an initial examination at the syntactic level. All the issues found in this level are technical in nature. The issues are lack of policy for use of unauthorised software; lack of guidelines for acceptance of new systems; lack of intrusion detection systems; lack of assessment for security vulnerabilities; lack of guidelines for systems audit.

7.5.5 Analysis of empiric layer

As shown in Table 7.5.1, the case study presented two issues that needed an initial examination at the empiric level. First, there is lack of guidelines for recording and quantifying security breaches. Second, internet bandwidth is small and expensive.

7.5.6 Analysis of the physical world layer

As shown in Table 7.5.1, the case study presented four issues that needed an initial analysis at the physical level. First, Security guards are illiterate and cannot use IT equipment. Second, fewer employees have access to computers. Third, employees allow relatives to use computers belong to their organisation. Fourth, computers are not physically locked.

7.6 Using the semiotic process model to evaluate the framework for information security culture

In this section, the findings from Section 7.5 were used to evaluate the proposed framework for information security culture from Section 6.2. This is done as follows: In Figure 7.6.1 the semiotic based framework for information security culture was presented developed in Section 7.4. Based on these semiotic layers the solutions identified in Section 7.5 were matched against the recommendations in Section 6.2. This provides the triangulation necessary to validate the information security culture framework. Table 7.6.1 shows the matching of the solutions against the recommendations. Figure 7.6.2 shows the link between Figures 7.6.1 and 6.3.1.

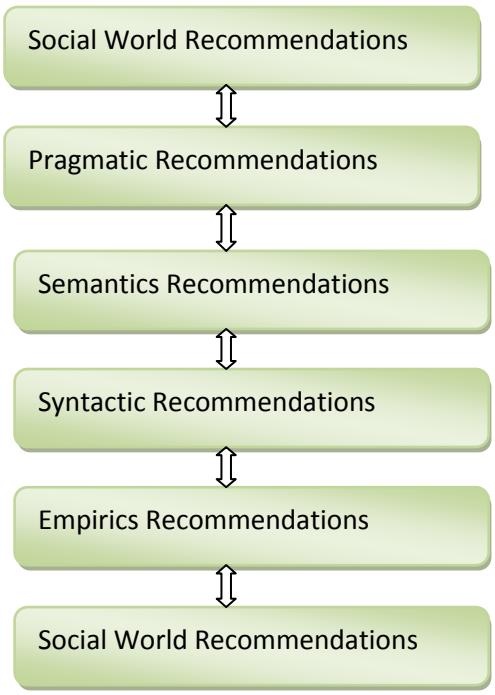

Figure 7.6.1: The Semiotic Based Framework for Information Security Culture

Table 7.6.1: Mapping Solution in Section 7.5 to Recommendations in Section 6.2

Semiotic Layer	Solution (Section 7.5)	Recommendations (Section 6.2)
Social World	Education, Training and Awareness Policy	(N1) Education and Awareness
	Standards and Best Practices Adaption Policy	(T1) Benchmarking Information Security Governance
	Compliance Policy	(C5) Regulatory Conformity
	Employee Security Policy	(C10) Personnel Security
	Corporate Governance	(O1) Corporate Governance
Pragmatics	Communication and Web Policy	(C2) Internet and E-mail
	Documentation Policy	(C1) Policy for Data Security
	Access Control Policy	(C6) Access Management
	Confidential Information Policy	(C10) Personnel Security
Semantics	Review and Evaluation Policy	(O2) Policy Creation and Enforcement
	Business Continuity Policy	(O3) Business Sustainability
	Employees Security Policy	(C10) Personnel Security
Syntactics	Use of Unauthorised Software Policy	(T1) Benchmarking Information Security Governance
	New Systems Acceptance Policy	(C3) Technical Controls
	Assurance Policy	(T3) Adopting Open Source Assurance Tools
	Vulnerability Assessment Policy	(C4) Vulnerability Assessment
	Systems Auditing Policy	(C5) Regulatory Conformity
Empirics	Security Incidence Policy	(C7) Control of Data Security Disaster
	Corporate Governance	(O1) Corporate Governance
Physical World	Education, training and awareness Policy	(N1) Education and Awareness
	Corporate Governance	(O1) Corporate Governance
	Employees Security Policy	(C10) Personnel Security
	Equipment Policy	(C8) Security of Building

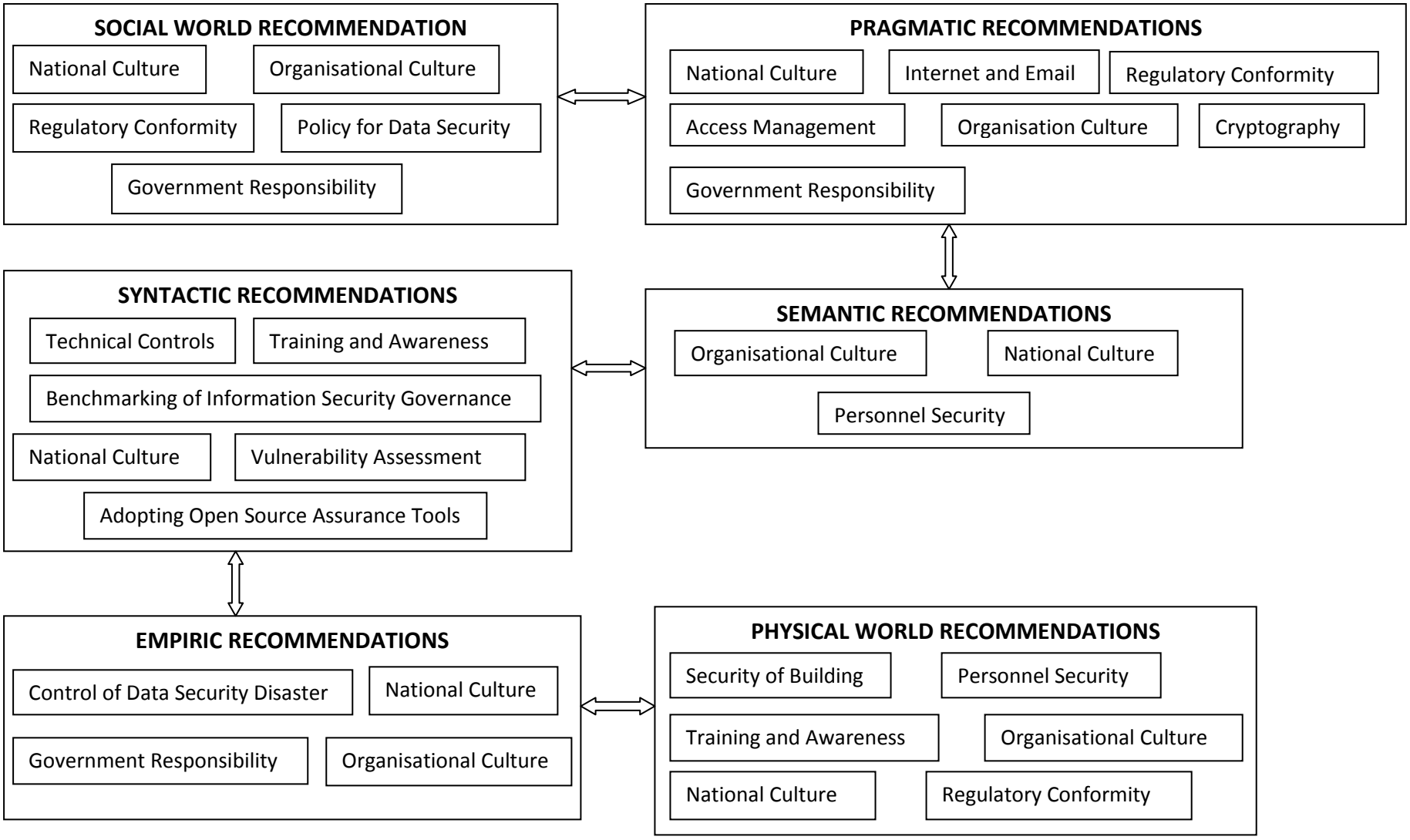

Figure 7.6.2: Linking Figure 6.3.1 to Figure 7.6.1

7.7 Conclusion

This chapter began with the explanation of the semiotic framework. Next, the semiotic framework was mapped against the national culture dimensions based on the GLOBE Project. Then, a semiotic diagnostic framework was proposed. Furthermore, a semiotic process model for improving information security governance was presented. The process model was then used for evaluation of the proposed framework of information security culture in Chapter 6. The semiotic based evaluation of the information security culture framework ensured a creation of a robust framework and integrated both social and technical solutions due to being grounded by the framework of organisational semiotics. The semiotic based framework for information security culture has enabled to find solutions for problems found in other layers by iterating through the layers. This was evidently seen by the use of cultural solutions in different layers. Therefore this chapter answer the research questions RQ4 and RQM.

The next chapter, Chapter 8, presents the conclusion of the thesis.

CHAPTER 8

8 CONCLUSION

8.1 Introduction

This chapter concludes the thesis. It discusses the questions addressed in this research. Next it gives a summary of contributions. Then it provides the implications for academia and organisational practice. Next it provides the limitation of research and finally provides recommendation for future research.

8.2 Questions addressed in this research

This thesis addresses the following research question:

What organisational factors need to be tackled or managed to develop and implement effective information security governance in the context of Zanzibar?

To address this question, an in-depth investigation of information security practices and complex societal issues facing information security governance in Zanzibar was conducted in the context of an interpretive case study. Data collection and analysis was guided by both qualitative and quantitative approaches. Two recommendations were made through a framework for information security culture and a semiotic process model for enhancement of information security governance.

The research question was examined by addressing the four very specific sub-questions below:

RQ1. *What are the existing information security strategies in literature?*

This question was addressed in Sections 2.4 and 2.5. Various strategies and approaches currently suggested in literature were reviewed, and it was revealed that strategy and

approach are country or organisation specific. Organisations must tailor an adapted strategy or approach to suit their requirement and culture. It was recommended that a new taxonomy is needed that incorporates social and technical issues in information security governance.

RQ2. *What is the current state of information security governance in non-profit organisations in the context of Zanzibar?*

This question was addressed in Chapter 4, which presented the findings of the data presenting the state of information security governance in ten public organisations in Zanzibar. It was revealed that:

- The organisations had varied level of security.
- Information security management is ad hoc and poorly governed.
- Organisations lack skilled personnel in information security.
- Policies are not reviewed or communicated to employees.
- Various controls such as vulnerability assessment and business continuity planning are not carried out or tested.
- Various controls such as monitoring and quantification of security incidents and network operations lack guidelines and policies.
- Contracts of employees lacked item specific to information security.
- Organisations have not implemented intrusion detection/protection systems.
- Employees lack regular training and awareness in information security.
- Security breaches were not severe and had little financial impact.

RQ3. *What are the cultural factors that impact upon information security governance in non-profit organisations in the context of Zanzibar?*

This question was addressed in Chapter 5, which presented the findings of the data demonstrating the cultural factors that impact upon information security management in non-profit organisations. Findings revealed that the cultural factors that influenced the governance of information security in the context of Zanzibar. Dimensions of national culture that influence the management of information security are Power Distance, Uncertainty Avoidance, In-Group Collectivism, and Future Orientation. In the case study, power is not shared equally; society does not seek orderliness or laws to cover situations in their daily lives; society take pride in their family or organisations; and society is not planning for the future. Organisational culture has little influence on management of

information security. Organisational culture is dominated by hierarchy culture, where success is determined by low cost, which explains the lack of fund for information security program.

RQ4. *How can non-profit organisations improve their information security governance in the context of Zanzibar?*

This question was addressed in Chapter 6, which presented a framework for information security culture. The framework will improve the governance of information security in the non-profit organisations in the context of Zanzibar. Chapter 7 presented an evaluation of the framework by grounding with the theory of semiotics. Semiotics helps to evaluate the framework for information security culture by providing much deeper analysis of information security in the case study. A process model for information security governance was developed for use in the evaluation of the framework.

8.3 Research contributions

The main contribution in this research is the semiotic process model for evaluating information security framework for non-profit organisations in the developing countries. By grounding the process model through the theory of semiotics, information security management in a non-profit organisation was analysed intensely through six layers of norms. The proposed process model was able to integrate both social and technical issues in evaluating information security management in a non-profit organisation. The model is adaptable to the need and environment of any organisation in the world. Prior to this research, there was no study which specifically grounded the theory of semiotics to model information security management in a developing country's environment. (Section 7.5)

Other contributions of the thesis are:

1. The research adds to the body of knowledge an important literature in the information security governance, requirements and procedures of non-profit organisations in the developing countries.

2. The research provides significant empirical evidence on the shortcomings of information security governance in ten public sector's non-profit organisations. (Chapter 4)

   A case study covering the public sector, provided in depth empirical data about the issues and influences on governing information security in ten non-profit

organisations. This data presented significant information, which was previously unknown in the context of Zanzibar. This research produced empirical data by adapting ISO 27002 best practices in information security governance and OWASP standard for web security.

3. The research presented significant empirical data on the national and organisational culture that was previously unknown in the context of Zanzibar. This study contributes new insights into the influence of culture in the management of information security. (Chapter 5)
   This research produced empirical data by adapting studies from the GLOBE Project and Competing Values Framework.

4. A framework for information security culture was recommended that will enhance information security governance in non-profit organisations. (Section 6.3)

5. A mapping between semiotic framework and national culture dimensions was provided that shows how each layer of the semiotic framework is influenced by national culture. This is a new insight when adapting the process model to other countries. (Section 7.3)

6. A framework for information security culture based on semiotic evaluation. (Section 7.6)

8.4 Research implications

The study has revealed insightful information on the governance of information security in non-profit organisations in a developing country context. It also identifies the cultural factors that impact the implementation of information security management in non-profit organisations in the context of a developing country, together with a framework and a semiotic process model for enhancing the management of information security.

The research can benefit the information security professionals and government policy makers by gaining insight into practices of management of information security in non-profit organisations and how to improve information security by implementing the proposed framework and process model.

Also, the study has revealed that the theory of semiotics can be used to analyse and improve information security where organisations face both social and technical issues in

their operations. Getting insights into cultural factors that influence management of information security can have significant contributions in the successful implementation of information assurance in non-profit organisations.

8.5 Research limitations

The research was conducted in non-profit organisations that belong to the public sector in the context of Zanzibar. Ten organisations were involved in the Phase I and nine organisations were involved in the Phase II of the research. Organisations were in different fields of services. Two of the organisations were larger in size compared to the others. Organisations were selected based on adoption of information systems in their services. Investigation on cultural issues may be biased due to participants being educated, work in the public sector and may be afraid to speak the truth. The impact of bias was minimised by using random selection of participants and assuring anonymity for participants.

The research employed both qualitative and quantitative approaches. The size of the research population was small and specific so it will be inappropriate to generalise on research findings, but the findings have provided useful insights for future work. Research aimed was to get a deeper understanding of issues facing information security rather than generalised. The reader will be able to take the information provided in this research and use it to help solve problems specific to their own environment. The research depends on the work of Stamper (1973), House et al (2004), Cameron and Quinn (1999) and BSI (2007).

8.6 Validation of the framework for information security culture

The framework for information security culture has been validated via the theory of semiotics in Chapter 7. To further validate the applicability in practice within the socio-cultural context of Zanzibar (or any other country where the framework would be applied) it will be necessary to instantiate the framework for instance in the form of policy documents or direct guidelines tailored against the organisations. Then, the framework would be deployed in a non-profit organisation in Zanzibar for a certain period of time, such as six months. An investigation is needed before and after six months of its implementation to assess the success of the framework. A further approach to validate the framework is to implement it in a non-profit organisation outside Zanzibar. In this approach cultural solutions should be adapted to suit the environment wherein the

organisation resides. An investigation is needed to assess the applicability of the framework before and after its deployment for a certain period of time.

For instance in the case of the State University of Zanzibar, the researcher will have a discussion with the university's Management Committee in order to get authorisation to deploy the framework at the university and investigate its applicability. If the framework is successfully deployed at the university, then it could be deployed to other non-profit organisations in Zanzibar.

8.7 Future research

The future research can look into developing the proposed framework and process model further. More research needs to investigate information security governance in non-profit organisations not belonging to public sector in the context of a developing country. The future research can look into the possibility of implementing semiotic diagnostic to secure Cloud Computing and Virtual World applications for usage in the non-profit sector. Other future research could investigate the validity of the framework developed in this thesis in Zanzibar or another developing country or in a private non-profit organisation. Also, future research could investigate the comparison of the applicability of the framework in rich developing countries versus poor developing countries. Furthermore, the future research could investigate the impact of culture on management of information security in a developed country context.

In this project, an exploratory case study was used. Further research could look at the application of an exploratory case study research as a potentially research approach to investigate problems outside information security in the non-profit sector. Grounding theory technique could be used in further research to strengthen data analysis in such a project.

Further research can look at challenges of enforcing law involving crimes on information systems and users of information systems in a developing country environment. Also, future research can investigate how to quantify information security breaches in a developing country environment. In addition, future research can look at usability factor of biometrics in a developing country view with a focus on social issues. Finally, further studies could be involved in developing a framework for benchmarking of information security governance in the context of a developing country.

8.8 Conclusion

This chapter concludes the thesis. This research has provided meaningful understanding of information security governance of non-profit organisations in the context of a developing country. A framework for information security culture has been recommended for effective information security governance in the non-profit organisations. The chapter discussed contributions of the research to the body of knowledge, implications of research and future works. By reading this work organisations in the developing countries could have an initial point of reference for their security requirements.

REFERENCES

Abu-Musa, A. (2010) 'Information security governance in Saudi organizations: an empirical study', *Information Management & Computer Security*, 18(4), pp.226-276 *Emerald* [Online]. Available at: http://www.emeraldinsight.com (Accessed: 09 May 2011)

ACCA (2012) *Not-for-profit.* Association of Chartered Certified Accountants. Available at: http://www.accaglobal.org.uk/content/dam/acca/global/pdf/3244839.pdf. (Accessed on 12 November 2012)

Aguilera, R. V. and Jackson, G. (2010) 'Comparative and international corporate governance', *The Academy of Management Annals,* 4(1), pp. 485-556.

Alberts, C. and Dorofee, A. (2003) *Managing information security risks, the OCTAVE approach.* New York, USA: Addison-Wesley.

Albirini, A. (2006) 'Teachers attitudes toward information and communication technologies: the case of Syrian EFL teachers', *Computer and Education*, 47 (4), pp. 373-398.

Alreck, P.L. and Settle, R.B. (1995) *The Survey Research Handbook*, 2nd edition. Chicago: Irwin.

Allen, R. E. (1991) *The concise Oxford dictionary of current English,* 8th Edition. Oxford: Clarendon Press.

Andersen, P. B. (2001) 'What semiotics can and cannot do for HCI', *Knowledge-Base Systems,* 14, pp.419-424.

Anthes, G. (2004) 'Model Mania', *Computer World* (*US*), 38(10), pp. 41-44.

Anttila, J. (2007) ‘Reinforcing business leaders’ role in striving for information security’, CIS’07 Conference, Harbin, China 15-19 December 2007.

Anttila, J. and Kajava, J. (2010) ‘Challenging IS and ISM Standardization for Business Benefits’, 2010 International Conference on Availability, Reliability and Security, Krakow, Poland 15-18 February 2010.

Arraj, V. (2010) *ITIL: The Basics,* Compliance Process Partners, LLC., APM Group Limited.

Ashkanasy, N., Gupta, V., Mayfield, M. S. and Trevor-Roberts, E. (2004) ‘Future orientation’ in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd pp.282-342.

Bakari, J., Tarimo, C., Yngström, L, and Magnusson, C., (2005) ‘State of ICT Security Management in the Institutions of Higher Learning in Developing Countries: Tanzania Case Study’, Fifth IEEE International Conference on Advanced Learning Technologies *(ICALT'05),* Kaohsiung, Taiwan, July 05-July 05.

BBC (2006) *Online banking fraud 'up 8,000%'*. Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/6177555.stm. (Accessed: 10 January 2011)

Benbasat, I., Goldstein, D. K., and Mead, M. (1987) ‘The case research strategy in studies of information systems’, *MIS Quarterly*, 11(3), pp. 369–386.

Bharvada, K. (2002) ‘Electronic signature, biometrics and PKI in the UK’, *International Review of Law Computers & Technology*, 16(3), pp. 265-275.

Bhatnagar, S. (2000) ‘Social implication of information and communication technology in developing countries: lessons from Asian success stories’, *EJISDC*, 1(4), pp. 1-9.

Bishop, M. (2003) *Computer Security: Art and Science*. Addison- Wesley.

Blair, M. M. (1995) *Ownership and control: rethinking corporate governance for the twenty first century*. Washington, DC: Brookings Institute.

Blythe, S. E. (2005) 'Digital signature law of the United Nations, European Union, United Kingdom and United States: Promotion of growth in E-commerce with enhanced security', *Richmond Journal of Law and Technology*, 11(2), pp.6-8. Available at: http://jolt.richmond.edu/v11i2/article6.pdf (Accessed: 21 August 2012).

Brake, J. (2003) 'Small Business Security Needs for the Changing Face of Small Business', in Dimopoulos, V., Furnell, S., Jennex, M. and Kritharas, I. (2004) *Approaches to IT security in small and medium enterprises*, 2nd Australian Information Security Management Conference, pp. 73-82, Perth, Australia, 26th November.

Brent, B. and Mshigeni, D. (2004), "Terrorism in Context: Race, Religion, Party, and Violent Conflict in Zanzibar", *The American Sociologist*, 35(2), pp. 60-74.

BSI (2005) *ISO/IEC 27001:2005 Information technology – security techniques – information security management systems – requirements*. British Standard Institute.

BSI (2007) *ISO/EIC 27002:2005 Information technology – Security techniques – Code of practice for information security management*. British Standard Institute.

BSI (2008) *ISO/EIC 27005:2008 Information technology — Security techniques — Information security risk management*. British Standard Institute.

Butler, K., McLaughlin, S., and McDaniel, P. (2008) 'Rootkit-resistant disks', Proceedings of 15th ACM Conference on Computer and Communication Security, Alexandria, Virginia, USA, October 2008.

BYU (2008) *Information Security Plan*. Brigham Young University. Available at: http://www.byui.edu/it/security/2008SecurityPlan.pdf. (Accessed on: 20 December 2010)

Cabinet Office (2009) *Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space*. Available at http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf. (Accessed on: (11 November 2010).

Cameron, K. S. and Quinn, R. E. (1999). *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework.* Reading, Massachusetts: Addison-Wesley

Cameron, K. S. and Quinn, R. E. (2006) *Diagnosing and Changing Organizational Culture: Based on the Competing Values Framework.* San Francisco, USA: Jossey-Bass.

Carl, D., Gupta, V., and Javidan, M. (2004) 'Power distance' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp.513-563.

Casmir, R., Yngstrom, L. (2003) 'IT Security Readiness in Developing Countries: Tanzania Case Study' in Irvine, C. and Armstrong, H. (eds.) *Security education and critical infrastructures*. Norwell, Mass: Kluwer Academic Publisher. pp. 117-127.

CERT (2010) *2010 Cybersecurity watch survey: Cybercrime increasing faster than some company defences.* Software Engineering Institute, Carnegie Mellow. Available at: http://www.cert.org/archive/pdf/ecrimesummary10.pdf. (Accessed: 28 November 2013)

Chang, S. E. and Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106(3):345–361.

Chaturvedi, M., Gupta, M., and Bhattacharya, J. (2008) 'Cyber Security Infrastructure in India: A Study', *Emerging Technologies in E-Government*, pp. 70-84 *CSI Publication* [Online]. Available at: http://www.csi-sigegov.org/emerging_pdf/9_70-84.pdf (Accessed: 17 September 2011).

Chaula, A., Yngstrm, L., and Kowalski, S. (2006) 'Technology as a tool for fighting poverty: How culture in the developing world affect the security of information systems', Proceedings of the 4th IEEE International Workshop on Technology for Education in Developing Countries *(TEDC06)*. Iringa, Tanzania, 10-12 July 2006.

Cheang, S. (2009) 'Conceptual Model for Cybersecurity Readiness Assessment For Public Institutions in Developing Country: Cambodia', 2009 Fourth International Conference on Computer Science and Convergence Information Technology, Seol, South Korea, November 24-26.

Cheang, S., and Sang, S. (2009) 'State of Cybersecurity and the Roadmap to Secure Cyber Community in Cambodia', 2009 International Conference on Availability, Reliability and Security, Fukuoka, Japan, March 16-19.

CISCO (2010) *The impact of global security threats and trends on the enterprise.* Cisco Systems.

CLUSIF (2008) *Information systems threats and security practices in France*. CLUSIF. Available at http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008-en.pdf (Accessed: 02 November 2010)

CNSS (2010) *National Information Assurance Glossary*. Available at: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf. (Accessed: 04 July 2010)

CS (2010) *Report of the Commonwealth observer group: Tanzania general elections.* Available at: http://www.thecommonwealth.org/files/232431/FileName/FinalReport-TanzaniaCOG.pdf. (Accessed on 19 November 2012)

CSI (2011) *2010/2011 Computer Crime and Security Survey.* Computer Security Institute.

Coyle, B. (2004) *Risk awareness and corporate governance*, 2nd ed. Canterbury: Financial World Publishing.

Creswells, J. (1994) *Research design: qualitative & quantitative approaches.* London: Sage.

Creswell, J. W. (1998) *Qualitative Inquiry and research design: Choosing among five traditions*. Thousand Oaks, CA: Sage.

Creswell, J. (2009) *Research Design. Qualitative, Quantitative, and Mixed Methods Approaches.* 3rd Edn. Thousand Oaks, Calif.; London: Sage. Available at: http://gocsi.com/sites/default/files/uploads/FBI2006.pdf. (Accessed on 10 June 2

CSI (2006) *2006 CSI/FBI Computer Crime and Security Survey.* 010)

Dansguardian (2013) *True web content filtering for all.* Available at: http://dansguardian.org (Accessed: 07 April 2013).

David, J. (2002), 'Policy enforcement in the workplace', *Computers & Security*, 21(6), pp. 506-513.

De Luque, M. S. and Javidan, M. (2004) 'Uncertainty avoidance' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin (eds.). *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd pp.602-653.

Den Hartog, D. N. (2004) 'Assertiveness' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin (eds.). *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd pp. 395-436.

Denzin N. and Lincoln Y. (Eds.) (2000). Handbook of Qualitative Research. London: Sage Publication Inc.

Dhillon, G. (1995). Interpreting the Management of Information Systems Security. London: London School of Economics and Political Science.

Dhillon, G. and May, J. (2006) 'Interpreting security in human computer interactions: a semiotic analysis', in Zhang, P. and Galletta, D. (eds.). *Human-Computer Interaction and Management Information Systems – Foundations.* New York: M. E. Sharpe, Inc. pp. 281-291.

Dhillon, G. and Torkzadeh (2006) 'Value-focused assessment of information system security in organizations', *Information Systems Journal*, 16(3), pp. 293–314.

Dickson, M., BeShears, R., and Gupta, V. (2004) 'The impact of societal culture and industry on organisational culture: theoretical explainations', in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 74-90.

Doherty, N. and Fulford, H. (2005) 'Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis', *Information Resources Management Journal*, 18(4), pp. 21-39.

Donaldson, L. (1993), *Anti-management theories of organization: a critique of paradigm proliferation*. Cambridge: Cambridge University Press.

Doolin, B. (1996) 'Alternative views of case research in information systems', *Australian Journal of Information Systems, 3*(2), pp. 21-29.

Eisenhardt, K. M. (1989) 'Building theories from case study research', *The Academy of Management Review*, 14(4), pp.532–550.

Emrich, C., Denmark, F. and Den Hartog, D. N. (2004) 'Cross-cultural differences in gender egalitarianism' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 343-394.

Ernst & Young (2009) *Outpacing change: Ernst & Young's 12th annual global information security survey*. Ernst & Young.

Fink, A. (2002) *The survey kit*. 2nd ed. Thousand Oaks, California: Sage

Fisher, T. (2013) Ophcrack v3.4.0 (LiveCD v3.4.0). Available at: http://pcsupport.about.com/od/toolsofthetrade/gr/ophcrack.htm. (Accessed: 09 January 2013)

French, T., Liu, K. and Springett, M. (2006) 'Towards an e-service semiotic trust framework', *Action in Language, Organisations and information Systems,* pp. 175-193.

Fourie, L., C., H. (2003) 'The management of Information Security- a South Africa case study', *South Africa Journal of Business Management,* vol. 34(2), pp.19-29.

Gazendam, H. (2004) 'Organizational semiotics: a state of the art report', *Semiotix,* 1(1). Available at: http://www.bdk.rug.nl/medewerkers/h.w.m.gazendam/WebBDK/Documents/2004/Semiotix%20Organizational%20Semiotics%20Introduction.pdf (Accessed: 11 December 2012)

Gelfand, M., Bhawuk, D., Nishii, L. H. and Bechtold, D. J. (2004) 'Individualism and Collectivism' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp.437-512.

Gerber, G., von Solms, R. and Overbeek, P. (2001) 'Formalizing information security requirements', *Information Management & Computer Security,* 9(1), pp.32-37. *Emerald*.

Gerber, M. and von Solms, R. (2005) 'Management of risk in the information age', *Computer and Security*, 24(1), pp. 16-30.

Glaser, T. D. (2009) *Culture and information security: outsourcing IT services in China*. PhD thesis. Berlin, Technischen Universität Berlin.

Gottdiener, M. (1995) *Postmodern semiotics: material culture and the forms of postmodern life*, Oxford: Blackwell Publishers.

Graziano, A. and Raulin, M. (2007) *Research methods: a process of inquiry*. Boston, MA: Pearson Education, Inc.

Grovewell (2012) *World differences in business values and practices: overview of GLOBE research findings.* Available at: http://www.grovewell.com/pub-GLOBE-dimensions.html. (Accessed on 3rd April 2012)

Guba, E. G., & Lincoln, Y. S. (1994) 'Competing paradigms in qualitative research', in N. K. Denzin and Y. S. Lincoln (Eds.), *Handbook of qualitative research*. Thousand Oaks, CA: Sage. pp. 105-117.

Hall, E. (1976) *Beyond Culture*, Anchor Books, New York, NY.

Handy, C. B. (1995) *Gods of management: the changing work of organisations.* 4th edition. Oxford: Oxford University press.

Heiman, G. (1998) *Understanding research methods and statistics: an integrated introduction for psychology*. Boston: Houghton Mifflin Co Inc.

HHS (2012) *Health Information Privacy.* Available at http://www.hhs.gov (Accessed: January 30, 2012)

Hickson, D. J., Hinings, C. R., McMillan, J., and Schwitter. (1974) 'The culture-free context of organization structure: A tri-national comparison', *Sociology*, 8(1), pp. 59-80.

Hofstede, G. (1980), *Culture's consequences: International differences in work-related values.* London: Sage.

Hofstede, G. (1997) *Cultures and organizations: software of the mind*. London: Mc Graw Hill.

Hofstede, G. (2001) *Culture's consequences: comparing values, behaviors, institutions and organizations across nations.* 2nd Ed. Thousand Oaks, Calif: SAGE Publications.

Hofstede, G. (2010) *Cultures and organizations: software of the mind: international cooperation and its importance for survival.* London: Mc Graw Hill.

Hofstede, G. and Hofstede, G. J. (2005) *Cultures and organizations: software of the mind.* 2nd ed. New York: McGraw-Hill.

Holt, J. (2005) *A pragmatic guide to business process modelling*. Swindon: British Computer Society.

Hone, K. and Eloff, P. (2002) 'Information security policy – what do international information security standards say?' *Computers & Security*, 21(5), pp.402–409.

Hong, K. S., Chi, Y. P., Chao, L. R., and Tang, J. H. (2006) 'An empirical study of information security policy on information security elevation in Taiwan', *Information Management & Computer Security*, 14(2), pp.104–115.

HOR (2011) *Member profile*. Available at: http://www.zanzibarassembly.go.tz. (Accessed on 28 November 2011)

House, R. and Javidan, M. (2004) 'Overview of GLOBE', in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 9-48.

House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. (2004). *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd.

Howlett, T. (2005) *Open Source Security Tools: Practical Applications for Security.* Upper Saddle River, NJ: Pearson Education, Inc.

Im, G. P. and Baskerville, R. L. (2005) 'A longitudinal study of information system threat categories: The enduring problem of human error', *ACM SIGMIS Database*, 36(4), pp.68–79.

Insecure.org (2012) *NMAP free security scanner, tools & hacking resources.* Available at: http://insecure.org. (Accessed: 10th September 2012)

In Silico Biotechnologies (2012) *PasswordChkr.txt.* Available at: http://www.insilicobiotechnologies.com/tutorials/PasswdChkr.txt. (Accessed: 8th September 2012)

ISO/IEC 15504 (2004) *Software process assessment.* Geneva: ISO.

ITGI (2007) *COBIT 4.1*. Rolling Meadows, IL: IT Governance Institute.

ITU (2005) *World summit on information society – Geneva 2003 – Tunis 2005*. Available at: http://www.itu.int. (Accessed: 02 July 2010)

ITU (2009) *Information society statistical profiles 2009*. Available at: http://www.itu.int. (Accessed: 02 July 2010)

Iivari, J. and Hirschheim, R. (1996) 'Analyzing information systems development: A comparison and analysis of eight is development', *Information Systems Journal*, 21(7), pp. 551–575.

Jamieson, S. (2004) 'Likert scales: how to (ab)use them', *Medical Education*, 38(12), pp. 1217-1218.

Javidan, M. (2004) 'Performance orientation' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 239-281.

Javidan, M. and House, R. (2001) 'Cultural acumen for the global manager: Lessons from project GLOBE', *Organization Dynamics*, 29(4), pp. 289–305.

Javidan, M., House, R. and Dorfman, P. (2004) 'A nontechnical summary of GLOBE findings', in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 29-48.

Juma, M. (2009) 'Exim Bank Installs System to Combat Fraudsters in ATMs', *The Citizen,* [Online]. Available at: http://allafrica.com/stories/200907271319.html (Accessed: 29 June 2010)

Kaaya, J. (2004). 'The emergency of e-government services in East Africa: tracking adoption patterns and associated factors', ICEC '04 Proceedings of Sixth International Conference on Electronic Commerce. ACM, pp. 438-445.

Kabasakal, H. and Bodul, M. (2004) 'Humane orientation in societies, organisations, and leader attributes' in House, R., Hanges, P. Javidan, M., Dorfman, P. and G. Vipin. *Culture, leadership and organizations: the GLOBE study of 62 societies*. London: Sage Publications Ltd. pp. 564-601.

Kadakia, Y. (2013) *Automated attack prevention.* Available at: http://www.acunetix.com/vulnerability-scanner/yashkadakia.pdf. (Accessed: 09 January 2013)

Kankanhalli, A., Teo, H., Tan, B. C. Y., and Wei, K. (2003) 'An integrative study of information systems security effectiveness', *International Journal of Information Management,* 23(2), pp. 139-154.

Kaplan, B. and Maxwell, J. (1994) *Qualitative Research Methods for Evaluating Computer Information Systems in Evaluating Health Care Information Systems: Methods and Applications*. Thousand Oaks: Sage.

Karokola, G. And Yngström, L. (2009) 'State of e-Government Development in the Developing World: Case of Tanzania – Security View', *Proceedings of the ICEG 2009* – 5th International Conference on e-Government, Suffolk University, Boston, USA. 19 – 20 October 2009.

Karokola, G. and Yngström, L. (2008) 'Lessons Learnt in the Process of Computerization, Automation and Management of ICT Security in the Developing World: A Case Study of the University of Dar Es Salaam, Tanzania'. *Proceedings of the ISSA 2008* - Innovative Minds Conference. Gauteng Region (Johannesburg), South Africa, 7-9 July 2008.

Khalfan, A. and Ashawaf, A. (2003) 'IS/IT outsourcing practice in the public health sector of Kuwait a contingency approach', *Logistic information Management*, 16(3/4), pp.215–228.

Kimwele, M., Mwangi, W., Kimani, S. (2010) 'Adoption of Information Technology Security: Case Study of Kenyan Small and Medium Enterprises (SMEs)', *Journal of Applied and Theoretical Information Technology*, 18(2), pp. 1-11 [Online]. Available at: http://www.jatit.org/volumes/research-papers/Vol18No2/1Vol18No2.pdf (Accessed: 13 October 2011)

Kimwele, M., Mwangi, W., Kimani, S. (2011) 'Information Technology (IT) Security Framework for Kenyan Small and Medium Enterprises (SMEs)' *International Journal of Computer Science and Security*, 5(1), pp.39-53 *Computer Science Journals* [Online]. Available at: http://cscjournals.org/csc/manuscript/Journals/IJCSS/volume5/Issue1/IJCSS-407.pdf (Accessed: 10 October 2011)

Klein, H. K., and Myers, M. D. (1999) 'A set of principles for conducting and evaluating interpretive field studies in information systems', *Management Information Systems Quarterly, 23*(1), pp. 67-94.

Kritzinger, E. and Smith, E. (2008) 'Information security management: an information security retrieval and awareness model for industry', *Computer and Security*, 27(5-6), pp. 224-231.

Kumar, R. (2005) *Research methodology: a step-by-step guide for beginners.* 2nd Ed. London: SAGE Publications Ltd.

Lacey, D. and James, B. (2010) *Review of availability of advice on security for small/medium sized organisations.* Available at: http://www.ico.org.uk/upload/documents/library/corporate/research_and_reports/review_availability_of_%20security_advice_for_sme.pdf. (Accessed: 29 November 2013)

Lee, W. (1997) 'A deterrent measure against computer crime: knowledge-based risk-analytic audit', *Singapore Management Review*, January, pp. 19-45.

Li, W., Liu, K., Li, S. and Yang, H. (2008) 'Normative modelling for personalised clinical pathway using organizational semiotics methods', *2008 International Symposium on Computer Science and Computational Technology*. Shangai, China 20-22 Dec. 2008.

Liu, K. (2000) *Semiotics in information systems engineering*, Cambridge, UK: Cambridge University Press.

Liu, K. and Xie, Z. (2002) 'Semiotics for information systems engineering – reduce the gap between specification, design, and implementation', 1st Int. Workshop on Interpretative Approaches to Information Systems & Computing Researc. Brunel University, UK, 25-27 July 2002.

Lord, R., and Maher, K. J. (1991) *Leadership and information processing: Linking perceptions and performance.* Boston: Unwin-Everyman.

Luthy, D. and Forcht, K. (2006) 'Laws regulations affecting information management and frameworks for assessing compliance', *Information Management & computer Security*, 14(2), pp. 155-166.

Lyons, M. and Hocking, S. (2000) *Dimensions of Australia's third sector*. Sydney, Australia: Centre for Australian Community Organisations and Management.

MAPAS (2012) *World Map.* Available at: http://mapas.owje.com/maps/3800_zanzibar-and-pemba-islands-political-map.html.

Martens, K. (2002) 'Mission impossible? Defining nongovernmental organizations', *Voluntas, International Journal of Voluntary and Nonprofit Organizations*, 13(3), pp. 271–285.

McClelland, D. C. (1985) *Human motivation.* Glenview, IL: Scott, Foresman.

Morgan, G., and Smircich, L. (1980) 'The case for qualitative research', *The Academy of Management Review, 5*(4), pp. 491-500.

Morse, J. M. (1994) 'Designing funded qualitative research', in N. K. Denzin and Y. S. Lincoln (Eds.), *Handbook of qualitative research*. Thousand Oaks, CA: Sage. pp. 220-233.

Moustakas, E., Ranganathan, C., and Duquenoy, P. (2005) 'Combating spam through legislation: a comparative analysis of us and European approaches', Proceedings of the Second Conference on Email and Anti-Spam. Stanford University, Stanford, CA. Available at: http://www.ceas.cc/2005/papers/146.pdf (Accessed: 13 January 2011).

Mundy, D and Musa, B. (2010) 'Towards a Framework for e-Government Development in Nigeria' *Electronic Journal of e-Government*, 8(2), pp.148-161 *Academic Conferences Ltd* [Online]. Available at: http://www.ejeg.com/volume8/issue2 (Accessed: 16 August 2011).

Mutarubukwa, A. (2010) Concern as hackers mess up crucial websites. *The Citizen*, 29 January [Online]. Available at: http://allafrica.com/stories/201001290326.html (Accessed: 29 June 2010)

NBS (2010) *National Bureau of Statistics.* Available at http://www.nbs.go.tz/takwimu/references/Tanzania_in_Figures2010.pdf

Ndou, V. (2004) 'E-Government for developing countries: opportunities and challenges', *EJISDC*, 18(1), pp. 1-24 [Online]. Available at: http://www.ejisdc.org/ojs2/index.php/ejisdc/article/viewFile/110/110 (Accessed: 12 January 2011).

Nelson, K. (2004) *A multi-methodological examination of information and knowledge management (IKM) in business contexts.* PhD thesis. Centre for Information Technology Innovation, Queensland University of Technology.

Neuman, W. L. (1997) *Social research methods: Qualitative and quantitative approaches*. Boston: Allyn and Bacon.

Ngo, L., Zhou, W., and Warren, M. (2005) 'Understanding transition towards information security culture change', *Proceedings of the third Australian information security management conference.* Perth, Australia 30 September 2005.

NHS Western Cheshire (2010) *ICT Security Strategy*. Available at: http://www.wcheshirepct.nhs.uk. (Accessed on: 10 December 2010)

Nielsen, S. K. (2012) "The implementation of an information system in a non-profit organisation in a developing country – Challenges and essential factors to take into

consideration in the preliminary work and implementation process", *Bachelor Thesis*. Department of Economics and Business, Aarhus University, Denmark.

NISC (2010) *Information security strategy for protecting the nation*. Available at http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf. (Accessed on: 21 November 2010)

Nishimura, T. and Sato, H. (2009) 'Analysis of a Security Incident of Open Source Middleware', *SAINT***.** Bellevue, Washington, USA, July 20-July 24 2009.

NISS (2007) *Republic of Mauritius*: *National ICP strategic plan 2007-2011*. Available at: http://www.gov.mu/portal/goc/telecomit/files/NISS.pdf. (Accessed on: 10 November 2010)

NIST (1996) *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Available at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. (Accessed: 20 February 2011)

NIST (1998) *Information technology security training requirements: a role and performance-based model*. Available at: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf. (Accessed: 21 February 2011)

NL- Aid (2012) *Tanzania: UAMSHO debate – is it religion, politics or a disease?* Available at: http://www.nl-aid.org/continent/sub-saharan-africa/tanzania-uamsho-debate-is-it-religion-politics-or-a-disease/ (Accessed: 23 November 2012)

Nour, M., AbdelRahman, A., and Fadlalla, A. (2007). A context-based integrative framework for e-government initiatives. *Government Information Quarterly*, 25(3), pp. 448–461.

OCAI (2010) *Organizational culture assessment instrument: public administration.* Available at: http://www.ocai-online.com. (Accessed: 25 November 2011)

OCGS (2011) *Zanzibar Statistical Abstract 2010*. Available at: http://www.ikuluzanzibar.go.tz/uploads/Zanzibar_Statistical_Abstract_2010.pdf (Accessed: 21 December 2011).

OD (2011) *Oxford Dictionaries.* Available at: http://oxforddictionaries.com.

Odedra, M. and Madon, S. (1993) *Information security policies and applications in the commonwealth developing countries.* Commonwealth Secretariat.

OECD (2011) *Implementing the OECD security guidelines.* Available at: http://www.oecd.org/internet/interneteconomy/2492747.pdf. (Accessed on 21 September 2011)

Orlikowski, W. J. and Baroudi, J. J. (1991) 'Studying information technology in organizations: research approaches and assumptions', *Information Systems Research, 2*(1), pp. 1-28.

OSI (2012) *The open source definition.* Available at: http://opensource.org/docs/definition.php. (Accessed: 12 January 2012)

OWASP (2010) *Open Web Application Security Project.* Available at: http://www.owasp.org. (Accessed: 18 November 2010)

Park, S. and Ruighaver, T. (2008) 'Strategic approach to information security in organisations', *2008 International Conference on Information Science and Security*, pp. 26-31, Seoul, Korea, 2008.

Parry, K. (1998) 'Grounded Theory and Social Process: A New Direction for Leadership

Research', *Leadership Quarterly*, 9(1), pp.85-105.

Pfleeger, C. (1997) 'The fundamentals of information security', *IEEE Software*, 14(1), pp.15 –16, 60.

Posthumus, S. and von Solms, R. (2004) 'A framework for the governance of information security', *Computer & Security*, 23(8), pp. 638-646.

POFEDP (2012) *Zanzibar budget speech 2011/2012.*

PS (2012) *Psychic science: random number generator & checker.* Available at: http://www.psychicscience.org/random.aspx (Accessed: 10 May 2012)

PWC (2008) '*BERR information security breaches survey 2008'.* Available at http://www.pwc.co.uk (Accessed: 01 June 2010)

PWC(2013) '*The global state of information security survey 2014*'. Available at http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-public-sector.pdf (Accessed: 25 November 2013)

Quinn, R. and Rohrbaugh, J. (1983) 'A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis', *Management Science*, 29(3), pp. 363-377.

Radianti, J. and Gonzalez, J. (2007) 'Understanding hidden information security threats: the vulnerability black market', *Proceedings of the 40th Hawaii International Conference on Systems Science*. Waikoloa, HI, January 2007.

Rambo, K., Liu, K. and Nakata, K. (2009) 'The socio-cultural factors influencing online female consumers in Saudi Arabia: an organisational semiotics perspective', *2009 International Conference on Computational Science and Engineering*. Vancouver, BC, 29-31 August 2009.

Robbins, S. P. (2005) *Essentials of organisational behaviour*. New York: Prentice Hall, 8th edition.

Sadallah, M. (2010) Maalim Seif for smooth transition of power in Z`bar. *The Guardian*, 30th October. [Online]. Available at: http://ippmedia.com (Accessed: 24 September 2012).

Sadallah, M. (2012) CCM: UAMSHO followers violate human rights in Zanzibar. *The Guardian*, 4th November 2012 [Online]. Available at: http://ippmedia.com (Accessed: 23 November 2012).

Salamon, L. M. and Anheier, H. K. (1996) *The international classification of nonprofit organizations - ICNPO. Revision 1.0* [Online]. Available at: http://www.ccss.jhu.edu/pdfs/CNP_Working_Papers/CNP_ WP19_INCPO_1996.pdf. (Accessed: 10 May 2010)

Saleh, M. S., Alrabiah, A. and Bakry S. H. (2007) 'A STOPE model for the investigation of compliance with ISO 17799-2005', *Information Management & Computer Security*, vol. 15(4), pp. 283-294.

Savvas, A. (2008). '*Monster.com users targeted by CV phishers*'. Available at: http://www.computerweekly.com/Articles/2008/07/15/231491/monster.com-users-targeted-by-cv-phishers.htm. (Accessed: 21 November 2010)

Schein, E. (2004) *Organizational culture and leadership.* San Francisco, Calif : Jossey-Bass.

Schlienger, T. and Teufel, S. (2002) 'Information Security Culture - The Socio-Cultural Dimension in Information Security Management', *IFIP TC11 International Conference on Information Security*, Cairo, Egypt, 7-9 May 2002.

Schlienger, T. and Teufel, S. (2003), "Information Security Culture - From Analysis to Change", in J.

Eloff, H. Venter, L. Labuschagne and M. Eloff, (Eds.) *IS South Africa -Proceedings of ISSA 2003,3rd Annual IS South Africa Conference*, Johannesburg, South Africa 9-11 July 2003.

Sedek, K., Osman, N., Osman, M., and Jusoff, K. (2009) 'Developing a secure web application using OWASP guidelines', *Computer and Information Science*, 2(4), pp. 137-143 [Online]. Available at: http://www.ccsenet.org/journal/index.php/cis/article/view/4279/3726 (Accessed: 20 February 2012).

Schneider, J. A. (2003) 'Small, Minority - Based Nonprofits in the Information Age', *Non-profit Management and Leadership* 13(4), pp.383-399.

Shaw, R., Chen, C., Harris, A., and Huang, H. (2009) 'The impact of information richness on information security awareness training effectiveness', *Computer and Education*, 52(1), pp. 92-100.

Sheng, S., Magnien, B., Kumaraguru, P.,Acquisti, A., Cranor, L., Hong, J.,and Nunge, E. (2007) 'Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish', in *Proceedings of the 2007 Symposium On Usable Privacy and Security.* Pittsburgh, PA, July 18-20. ACM Press.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010) 'Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions', *CHI 2010: Privacy Behaviors.* Atlanta, GA, April 10-15. ACM Press.

Simmons, C. and Burgess, L. (2000) 'Internet commerce, security risk analysis & small to medium enterprises', 5th CollECTer Conference on Electronic Commerce, Brisbane, Australia 13-14 December.

Singel, R. (2008, 1st March) *Fraudsters target facebook with phishing scam*. Available at: http://www.wired.com/politics/security/news/2008/01/facebook_phish (Accessed: 23 March 2012).

Singh A. & Lilja, D. (2010) 'Criteria and Methodology for GRC Platform Selection', *Information System Audit and Control Association Journal,* 1, [Online]. Available at: http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Documents/1001-criteria-and-methodology.pdf (Accessed: 25 February 2011).

Siphonen, M. and Willison, R. (2009) 'Information security management standards: problems and solutions', *Information and Management,* 46, pp. 267-270.

Siponen, M. and Oinas-Kukkonen, H. (2007) 'A review of information security issues and respective research contributions', *Database for Advances in Information System*, 38(1), pp.60–80.

Sjostrom, J., and Goldkuhl, G. (2003) 'The semiotics of user interfaces–a socio-pragmatic perspective', *6th International Workshop on Organizational Semiotics*, Reading, UK, 11-12 July 2003.

Skoudis, E. and Zeltser, L. (2003) *Malware: fighting malicious code,* NJ, USA: Prentice Hall PTR.

Snort (2013) *What is Snort?* Available at: http://snort.org (Accessed: 04 April 2013).

Stake, R. E. (1995) *The art of case study research*. Thousand Oaks, CA: Sage.

Stamper, R. (1973) *Information in business and administrative systems.* New York: John Wiley and Sons.

Stamper, R. Liu, K., Hafkamp, M. And Ades, Y. (2000) 'Understanding the roles of signs and norms in organisations', *Journal of Behaviour & Information Technology*, 19(1), pp. 15-27.

Straker, D. (2002) *Trompenaars' four diversity cultures*. Available at: http://changingminds.org/explanations/culture/trompenaars_four_cultures.htm (Accessed: 13 April 2012).

Sturgeon, W. (2007) *Botnets could eat the internet*. Available at: http://www.zdnet.com/botnets-could-eat-the-internet-3040149927/ (Accessed: 27 November 2013)

Sultani, A. (2011) 'Zanzibar to adopt e-government 2012', *Daily News*. [Online] Available at: http://dailynews.co.tz/business/?n=24431. (Accessed: 20 October 2011).

Suppiah-Shandre, H. (2002) 'Security - Top Priority For All', in Dimopoulos, V., Furnell, S., Jennex, M. and Kritharas, I. (2004) *Approaches to IT security in small and medium enterprises*, 2nd Australian Information Security Management Conference, pp. 73-82, Perth, Australia, 26th November.

SWATCH (2013) *The simple watcher of logfiles.* Available at: http://swatch.sourceforge.net (Accessed: 04 April 2013).

Szilagyi, A. D. and Wallance, M. J. (1990) *Organisational behaviour and performance.* 5th edition. Illinois: Scott, Foresman and Company.

Tarimo, C., Bakari, J., Yngström, L, and Kowalski, S. (2006), 'A Social-Technical View of ICT Security Issues, Trends, and Challenges: Towards a Culture of ICT Security- The Case of Tanzania', Proceedings of the ISSA 2006 from Insight to Foresight Conference,5-7 July 2006, Sandton, South Africa.

Tanzania. Communication Regulatory Authority Act 2003. Available at: http://polis.parliament.go.tz/PAMS/docs/12-2003.pdf (Accessed: 03 August 2011)

TCRA (2010) *Report on internet and data service in Tanzania: a supply-side survey*. Available at: http://www.tcra.go.tz/images/documents/reports/InternetDataSurveyScd.pdf (Accessed: 6 April 2011).

Tenable Network Security (2013) *NESSUS vulnerability scanner: fuelled by nessus professionalfeed. Available at:* http://www.tenable.com/products/nessus (Accessed: 04 April 2013).

Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005) 'The insider threat to information systems and the effectiveness of ISO17799', *Computers and Security*, vol. 24(6), pp. 472-484.

Tierney, W. (1996) 'Leadership and Post-modernism: on voice and the qualitative method', *Leadership Quarterly*, 7(3), pp.371-383.

Truecrypt (2012) *Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux.* Available at: http://www.truecrypt.com (Accessed: 9th September 2012)

United Nations, (2008) *Statistical Yearbook*. Fifty-third issue, pp.3. New York: United Nations. Available online at http://unstats.un.org/unsd/syb/syb52.pdf (Accessed: 8 July 2010).

UT (2007) *Information Technology Security Strategy*. Available at http://security.tennessee.edu/pdfs/ITSS.pdf. (Accessed on 12 November 2010)

Vander biesen, I. (2009) 'Social and Intercultural Relations in Nineteenth-Century Zanzibar: Dressed Identity', *African and Asian Studies,* 8(3), pp. 309-331. *BRILL*.

van Everdingen, Y. and Waarts, E. (2003) 'The effect of national culture on the adoption of innovations', *Marketing Letters*, 14(3), pp. 217-232.

von Solms, B. (2001) 'Corporate governance and information security', *Computer & Security*, 20(3), pp. 215-218.

Vroom, C. and von Solms, R. (2004) 'Towards information security behavioural compliance', *Computers & Security*, 23(3), pp.191–198.

von Solms, B. and von Solms, R. (2004a) 'The 10 deadly sins of information security management', *Computers & Security*, 23(5):371–376.

von Solms, R. and von Solms, B. (2004b) 'From policies to culture', *Computers & Security*, 23:275–279.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*. Chichester: Wiley.

Walsham, G. (1995a) 'The emergence of interpretivism in IS research', *Information Systems Research*, 6(4), pp. 376-394.

Walsham, G., (1995b), 'Interpretive Case Studies in IS Research: Nature and Method', *European Journal of Information Systems*, 4(2), pp.74-81. *Palgrave Macmillan.*

Whelan, T. and Wright, D. (1999) 'Methodology for cost-benefit analysis of web-based tele-learning: case study of the Bell Online Institute', *The American Journal of Distance Education*, 13(1), pp. 25-43.

Whitman, M. E. and Mattord, H. J. (2005) *Principles of information security*, 2nd Edition, Massachusetts: Course Technology.

Wolff, S. (2004) 'Analysis of documents and records' in Flick, U., Kardorff, V. E., and Steinke, I. (eds), *A companion to qualitative research.* London: Sage. pp. 284-290.

Yin, R. K. (2003) *Case study research: Design and methods.*3rd ed. Thousand Oaks, CA: Sage.

Zanzibar. Broadcasting Commission Act 1997. Zanzibar: Government Press.

Zanzibar. Censorship and Cinematographic Exhibition Act 2009. Zanzibar: Government Press.

Zanzibar. Copyright Act 2003. Zanzibar: Government Press.

Zanzibar. Criminal Procedure (Amendment) Act 2004. Zanzibar: Government Press.

Zanzibar. Industrial Property Act 2008. Zanzibar: Government Press.

Zanzibar. Penal Degree Act 6 of 2004. Zanzibar: Government Press.

Zanzibar. Public Service Act 2010. Zanzibar: Government Press.

Zimbra (2012a) *Zimbra collaboration suite : open source edition.* Available at: http://www.zimbra.com/products/zimbra-open-source.html. (Accessed: 6th September 2012)

Zimbra (2012b) *Zimbra collaboration suite 7.0 - open source edition: admin guide.* Available at: http://www.zimbra.com/community/documentation.html . (Accessed: 6th September 2012)

Zuccato, A. (2007) 'Holistic security management framework applied in electronic commerce', *Computers & Security*, vol. 26 (3), pp. 256-265.

APPENDICES

APPENDIX A: QUESTIONNAIRE I - INFORMATION SECURITY ASSESSMENT

(Phase I)

Management Staff

Respondent ID: ..... (For the researcher use) **Date:** .....

Organisation and Department: .....

Position: ......

Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	2	3	4	5

Number 1-5 represents your response to the statement. Please mark (√) on a box that you think represents most appropriate choice for your response.

Item	Statement	1	2	3	4	5
	Information security policy					
1	There is an information security policy for the organisation.					
2	Information security policy is conveyed to all employees.					
3	Information security policy is periodically reviewed.					
	Organisation of Information Security					
4	There is an information security committee in place.					
5	There is a budget for information security program.					
6	The organisation is capable of implements information security awareness program.					
7	The organisation defined and documented all information security roles.					
8	There is a restriction on the use of personal information processing resources such as laptops.					
9	There is some confidentiality or non-disclosure agreement for protection of information asset.					
10	There is some authorisation for use of confidential information.					
11	There is some procedure in place that specifies how to contact authority (e.g police).					
12	There is some contact with information security associations.					
13	The organisation conducts independent information security review.					
14	The organisation conducts information risk assessment when dealing with an outside party.					
15	The organisation addresses some security needs before giving customer access to organisation's assets.					
16	There is some agreement with third party involving accessing organisation's facilities.					
	Asset management					
17	There is an inventory of assets.					
18	The inventory of assets includes software assets.					
19	There is assets manager.					
20	There is information classification in the organisation.					
	Human resources security					
21	There is a training and awareness program periodically in information security.					
22	There is a disciplinary action against the non-compliant employee.					
23	Security roles and responsibilities are defined, documented, and conveyed to would be employees.					

Item	Statement	1	2	3	4	5
24	There is a background verification check for candidates of employment and third party.					
25	Terms and conditions of employment include an item about information security.					
26	All employees, contractors, and third party receive information security awareness training.					
27	All employees return organisation's assets upon termination of their employment.					
28	The access right to information assets is removed after employment termination.					
	Physical and Environmental Security					
29	There is a security perimeter to protect the area that contains information and information processing facilities.					
30	The office rooms and facilities have locks.					
31	There is an emergency generator.					
32	The ICT equipments are connected with Uninterrupted Power Supply unit (UPS).					
33	The cables are protected from interference.					
34	The organisation's equipment is maintained.					
35	The equipment is maintained according to supply recommendation.					
36	There is organisation's guideline on working off-site premises with organisation's equipment.					
37	There is a guideline on ICT equipment disposal or re-use.					
38	The organisation facilities are protected against damage from fire, flood, explosion, civil unrest, rainfall, lightning, and man-made disaster.					
39	The equipment is protected against theft and unauthorised access.					
	Access Control					
40	There is an access control policy.					
	Information systems acquisition, development and maintenance					
41	There is use of cryptographic control policy.					
	Information Security Incidents Management					
42	There is a reporting mechanism about information security incidence.					
	Business Continuity Management					
43	There is a business continuity plan in the event of a disaster.					
44	Business continuity plans include information security.					
	Compliance					
45	The organisation is in compliance with the legal requirement.					
46	There is a guideline to ensure intellectual properties rights.					
47	There is a guideline to ensure the protection of organisational records.					
48	There is a guideline to ensure data protection and privacy of personal information.					
49	There is a guideline on prevention of misuse of information processing facilities.					
50	There is a guideline on ensuring all security procedures are performed correctly to meet compliance with security policies and standards.					

Thank you very much indeed for your help!

APPENDIX B: QUESTIONNAIRE II - INFORMATION SECURITY ASSESSMENT

(Phase I)

IT Staff

Respondent ID :.....(for the researcher use) **Date:** .....

Organisation and Department: .....

Position: .....

Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	2	3	4	5

Number 1-5 represents your response to the statement. Please mark (√) on a box that you think represents most appropriate choice for your response.

Item	Statement	1	2	3	4	5
	Physical and Environmental Security					
1	There is a guideline on removal of equipment, information and software.					
	Human Resource security					
2	There are qualified network and system administrators.					
	Communication and Operations Management					
3	There is a separation of development, test, and operational facilities.					
4	There is a guideline for acceptance of new information systems.					
5	There is a policy for prohibiting the use of unauthorised software.					
6	There any backup policy for information and software.					
7	There is a network operational guideline.					
8	The security features, service levels, and management requirements of all network services have been identified and documented.					
9	There is a removable media guideline.					
10	There is some procedure for handling and storage of information.					
11	System documentation is protected against unauthorised access.					
12	There is information exchange policy.					
13	There is a guideline for physical media under transit which contains information.					
14	There is a policy to protect electronic messaging.					
15	There is a policy to protect information in electronic commerce passing over the public network.					
16	There is a policy to protect information involved in the on-line transaction.					
17	There is a guideline to keep audit logs recording user activities, exceptions, and information security events.					
18	There is a procedure to monitor system use.					
19	System administrator and system operator activities are logged.					
20	Clock is synchronized with agreed accurate time source.					
21	Employees and system activities are regularly monitored under existing legal framework.					
22	Use of resource in computer systems is monitored.					

Item	Statement	1	2	3	4	5
	Access Management					
23	There is a user password guideline.					
24	There is a review of user access rights periodically.					
25	There is a user guideline for selection and usage of password.					
26	There is a clear desk and clear screen policy.					
27	There is a policy for use of network services.					
28	Remote users are authenticated.					
29	There is automatic equipment identification in the network.					
30	There is separation of networks into domains according to function.					
31	There is a restriction on users' ability to connect to the network.					
32	There is routing implementation to enforce access control policy.					
33	There is an implementation of users' identification and authentication for access to organisation's information systems.					
34	There is a system to manage passwords.					
35	There is a guideline for system utilities usage.					
36	There is a guideline for session time-out.					
37	There is a guideline for connection time to information systems.					
38	There is access control policy.					
39	There is mobile computing policy.					
40	There is a tele-working guideline.					
	Information systems acquisition, development and maintenance					
41	Data input to organisation's information systems were validated.					
42	The security risk assessment is applied to ensure message integrity.					
43	There is a validation of data output from organisation's information systems.					
44	Encryption is used to protect sensitive information assets.					
45	There is cryptographic key management guideline.					
46	There are procedures for managing software installation on running systems.					
47	There is a restriction on access to program source code.					
48	There is a guideline protection of test data on running systems.					
49	There are procedures for implementing changes to running systems.					
50	Applications are reviewed after changes in operating systems.					
51	There is discouragement on modifying software packages supplied by vendors.					
52	Periodical technical vulnerabilities assessment is carried out, and actions are taken to address any found.					
	Information Security Incidents Management					
53	There is reporting mechanism for information security incidents.					
54	There is a guideline to quantify and monitor information security incidents.					
	Business Continuity Management					
55	Business continuity plans are tested in a regular basis.					
	Compliance					
56	There is a regular check on technical compliance.					
57	There is a guideline for information systems audit.					

Thank you very much indeed for your help!

APPENDIX C: QUESTIONNAIRE III - INFORMATION SECURITY ASSESSMENT (Phase I)

General Staff
Respondent ID: ..... (For the researcher use) **Date:** .....
Organisation and Department: .....
Position: .....

Strongly disagree	Disagree	Undecided	Agree	Strongly agree
1	2	3	4	5

Number 1-5 represents your response to the statement. Please mark (√) on a box that you think represents most appropriate choice for your response.

Item	Statement	1	2	3	4	5
	Information security policy					
1	There is an information security policy in place.					
2	I have read the Information security policy.					
3	Information security policy is periodically reviewed.					
	Organisation of Information Security					
4	I have signed confidentiality or non-disclosure agreement for protection of organisation's information assets.					
	Human Resource security					
5	There is a periodic awareness and training program in information security.					
6	There is a disciplinary action against the non-compliant employee.					
7	My background has been verified.					
8	I agreed and signed terms and conditions of employment that includes responsibilities for information security.					
9	I was provided with information security expectation of my position.					
10	I receive information security awareness training regularly.					
	Physical and Environmental Security					
11	Access to my office is through a door that has a lock.					
12	My desk and cabinet can be locked.					
13	I wear employee identity card all the time inside the organisation's building.					
	Communication and Operations Management					
14	There are rules for using electronic mail and Internet.					
15	I have only one role in my employment.					
	Access Control					
16	I am the only person who knows my password for access to organisation's information system.					
17	I use a screen saver that is password protected.					
18	I have read clear desk and clear screen policy.					
19	My password contains alphabets and numbers characters.					
	Information Systems Acquisition, Development and Maintenance					
20	I use encryption when sending sensitive information.					
	Information Security Incidents Management					
21	I know where to report information security incidents.					
	Business Continuity Management					
22	I am aware of organisation’s business continuity plans.					
	Compliance					
23	I am aware of organisation’s intellectual property policy.					
24	I am aware of organisation’s guidelines on retention and disposal of information.					
25	There is an organisation’s data protection and privacy policy.					

Thank you very much indeed for your help!

APPENDIX D: QUESTIONNAIRE IV – SECURITY ASSESSMENT OF WEBSITES (Phase I)

IT Staff

Respondent ID: ..... (For the researcher use)
Organisation and Department: .....
Position: .....
Date: .....
Organisation's website address: .....

Mark a box that represents your response.

Item	Statement	Yes	No	Don't know
1	Does the organisation host the website in-house?			
2	Is the website developed in-house?			
3	Is the website runs database queries?			
4	If the answer in 3 is yes, is there separate physical server for web and database?			
5	Is there the organisation's guideline for user id and password used in the website?			
6	Is there the organisation's guideline for displaying user data in the website?			
7	Is there a separate development, test, and production environments for web application?			
8	Does the organisation implement the current Open Web Application Security Project guidelines to protect its website?			
9	Do you test your web application for security vulnerabilities?			
10	Does the organisation have restriction on who is allowed to publish the web application to production environment?			
11	Does the organisation's website implement encryption?			
12	Does the organisation have guidelines on web application that involves in data collection or transmission?			
13	Does the organisation review web server logs for security incidents?			
14	Is there any periodic training in secure coding to organisation's developers?			
15	Is there any periodic security review of the organisation's website?			
16	Does the organisation in compliance with any web application security standard?			

Thank you very much indeed for your help!

APPENDIX E: INTERVIEW GUIDE I - THREAT ANALYSIS (PHASE I)

IT Staff

Respondent ID: ..... (For the researcher use) **Date:** .....

Organisation and Department: .....

Position: .....

1. What are the core services of organisation/department?

Item	Name of service
1	
2	
3	
4	

2. What is an approximate number of computers on the use in your organisation?

3. Is there an organisation's Local Area Network? If yes, what its size?

4. Is there an organisation's Wide Area Network?

5. Is there Internet connection?

6. Is there a wireless network?

7. Is there remote login access?

8. What is the percentage of the organisation's services are automated?

9. In your organisation, what would be damage due to loss of availability of information system?

Item	Information system	Damage
1		
2		
3		
4		

10. List all information security incidents occurred in your organisation in the last two years.

Item	Incident	Damage
1		
2		
3		
4		
5		

11. List the educational and professional qualifications of all IT staff.

Item	Qualifications	Number of Employees
1		
2		
3		
4		
5		

12. List all networking equipment your organisation is connected to.

Item	Equipment	Quantity
1		
2		
3		
4		
5		

12. List all software installed in the organisation's computers and servers for protecting the organisation against security breaches.

Item	Software
1	
2	
3	
4	
5	

13. What is a percentage of the total budget is allocated for information security?

14. Is there periodic virus scan?

15. Is there periodic anti-virus updates?

16. Do you attend a periodic information security awareness and training programs?

17. Is there a qualified information security professional among staff members?

18. Do you share the password of any system in the organisation with someone else?

19. Have you ever allow your organisation's computer to be used by your relative?

20. Have you ever suffered from computer virus/trojan/other malware?

21. If the answer is yes for question 20, list the names of virus/trojan/other malware and damage coursed?

Item	Virus/Trojan/Other malware	Damage
1		
2		
3		
4		
5		

22. Has anyone's email address ever been used to send emails to their contacts without their consent?

23. Have your organisation ever experienced the following effects due to information security breaches. Please select the appropriate effect from the list.

Effect	
Fraud and embezzlement	
Robbery and theft of ICT equipments	
Defamation	
Infringement of privacy	
Customer information leakage	
Hacking activities	
Denial of service	
System sabotage by employee	
Loss of information	
Website hijacking/defacing	

System	Possible Threats	Possible Vulnerabilities

Thank you very much indeed for your help!

APPENDIX F : QUESTIONNAIRE V – National Cultural Evaluation (Phase II)
Public Sector Employee
Respondent ID: ..... (For the researcher use) **Date:** .....
Organisation and Department: .....
Position: .....

Substantially Agree	Moderately Agree	Slightly Agree	Neither Disagree nor Agree	Slightly Disagree	Moderately Disagree	Substantially Disagree
1	**2**	**3**	**4**	**5**	**6**	**7**

Number 1-7 represents your response to the statement. Please mark (√) on a box that you think represents most appropriate choice for your response.

	Statement	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Followers are expected to obey their leaders without question.							
2	Followers should be expected to obey their leaders without question.							
3	Most people lead highly structured lives with few unexpected events.							
4	Most people should lead highly structured lives with few unexpected events.							
5	People are generally very tolerant of mistakes.							
6	People should be generally very tolerant of mistakes.							
7	Leaders encourage group loyalty even if individual goals suffer.							
8	Leaders should encourage group loyalty even if individual goals suffer.							
9	Employees feel great loyalty toward this organisation.							
10	Employees should feel great loyalty toward this organisation.							
11	People are generally dominant.							
12	People should be generally dominant.							
13	Boys are encouraged more than girls to attain a higher education.							
14	Boys should be encouraged more than girls to attain a higher education.							
15	More people live for the present than for the future.							
16	More people should live for the present than for the future.							
17	Students are encouraged to strive for continuously improved performance.							
18	Students should be encouraged to strive for continuously improved performance.							

Thank you very much indeed for your help!

APPENDIX G : QUESTIONNAIRE VI – Assessment of Organisational Culture (Phase II)

Public Sector Employee

Respondent ID: ..... (For the researcher use) **Date:** .....

Organisation and Department: .....

Position: .....

There are six questions in this questionnaire. Each question has four options. Divide 100 points among these four options depending on the extent to which each option is similar to your own organisation. There are two response columns, one labelled NOW as it represents the current situation and another labelled PREFFERED as it represents situation you think in five years.

1. Dominant Characteristics		**NOW**	**PREFERRED**
A	The organisation is very personal place. It is like an extended family. People seem to share a lot of themselves.		
B	The organisation is very dynamic and entrepreneurial place. People are willing to stick their necks out and take risks.		
C	The organization is very results-oriented. A major concern is getting the job done. People are very competitive and achievement-oriented.		
D	The organization is a very controlled and structured place. Formal procedures generally govern what people do.		
	TOTAL	**100**	**100**
2. Organisational Leadership		**NOW**	**PREFERRED**
A	The leadership in the organization is generally considered to exemplify mentoring, facilitating, or nurturing.		
B	The leadership in the organization is generally considered to exemplify entrepreneurship, innovation, or risk taking.		
C	The leadership in the organization is generally considered to exemplify a no-nonsense, aggressive, results-oriented focus.		
D	The leadership in the organization is generally considered to exemplify coordinating, organizing, or smooth-running efficiency.		
	TOTAL	**100**	**100**
3. Management of Employees		**NOW**	**PREFERRED**
A	The management style in the organization is characterized by teamwork, consensus, and participation.		
B	The management style in the organization is characterized by individual risk taking, innovation, freedom, and uniqueness.		
C	The management style in the organization is characterized by hard-driving competitiveness, high demands, and achievement.		
D	The management style in the organization is characterized by security of employment, conformity, predictability, and stability in relationships.		
	TOTAL	**100**	**100**

4. Organisational Glue		NOW	PREFERRED
A	The glue that holds the organization together is loyalty and mutual trust. Commitment to this organization runs high.		
B	The glue that holds the organization together is a commitment to innovation and development. There is an emphasis on being on the cutting edge.		
C	The glue that holds the organization together is an emphasis on achievement and goal accomplishment.		
D	The glue that holds the organization together is formal rules and policies. Maintaining a smooth-running organization is important.		
	TOTAL	**100**	**100**
5. Strategic Emphases		**NOW**	**PREFERRED**
A	The organization emphasizes human development. High trust, openness, and participation persist.		
B	The organization emphasizes acquiring new resources and creating new challenges. Trying new things and prospecting for opportunities are valued.		
C	The organization emphasizes competitive actions and achievement. Hitting stretch targets and winning in the marketplace are dominant.		
D	The organization emphasizes permanence and stability. Efficiency, control and smooth operations are important.		
	TOTAL	**100**	**100**
6. Criteria of Success		**NOW**	**PREFERRED**
A	The organization defines success on the basis of development of human resources, teamwork, employee commitment, and concern for people.		
B	The organization defines success on the basis of having the most unique or newest products. It is a product leader and innovator.		
C	The organization defines success on the basis of winning in the marketplace and outpacing the competition. Competitive market leadership is key.		
D	The organization defines success on the basis of efficiency. Dependable delivery, smooth scheduling and low-cost production are critical.		
	TOTAL	**100**	**100**

Thank you very much indeed for your help!

APPENDIX H: INTERVIEW GUIDE II – Complex Societal Issues Concerning Governance of Information Security (Phase II)

I would like to do an interview with you concerning the issues that face the governance of information security in your organisation. I would like you to answer according to your point of view and express your opinions. All the answers you give me will be confidential and only be used for the purpose of this study. I will only take your name for my record only.

Q1. What do you think about the usage of computers and internet in this organisation?

Q2. What do you think about the cooperation between IT staff and security staff?

Q3. What do you think about the confidentiality of information in this organisation?

Q4. Do you think employees trust each other in this organisation?

Q5. What do you think about policy enforcement and disciplinary action in this organisation?

Q6. What do you think about the communication between employees when problems are discovered and solved?

Q7. What do you think about the availability of funds for implementation of daily tasks in this organisation?

APPENDIX I: An Introduction Letter to Participants

Dear Sir/Madam

I am conducting a research at the University of Bedfordshire, focusing on potential solutions in relation to information security management. As a part of that research, your organisation has been selected as one of ten organisations in Zanzibar to participate as a case study.

Information presented by interviewees will only be used for the purpose of this research. In the description of results of this survey, no identification of individual persons will be made. Individual answers will be kept confidential. Your details will be taken for my records only.

Thank you in advance for your priceless time and thoughtfulness.

Yours faithfully

Hussein Shaaban
PhD Student, IRAC
University of Bedfordshire
Email: Hussein.Shaaban@beds.ac.uk